SECURITY NOW!

Transcript of Episode #557

Listener Feedback #232

Description: Leo and I discuss an interesting week of security news, including an update on Let's Encrypt's growth, the advance in encryption thanks to Edward Snowden, a clever bypass for Windows AppLocker, Opera's built-in VPN that isn't, more crypto ransomware evolution, fake DDoS extortionists, some DNSSEC follow-up, and 10 great questions and talking points from our 200,000-plus weekly listeners!

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-557.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-557-lq.mp3

SHOW TEASE: It's time for Security Now!, the show where we talk about the latest security news and information with my friend Steve Gibson. There is a lot of security news. Steve will talk about it. And we'll also, I'm liking this, we're going to get to some of your listener questions. And we're going to do some basics, some of the fundamentals, like should you use an antivirus? What's the difference between a NAT router and a firewall? We're going to explain - and how to avoid spam. We're going to explain all that and more, next on Security Now!.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 557, recorded Tuesday, April 26th, 2016: Your questions, Steve's answers, #232.

It's time for Security Now!, the show where we cover the security. What else can I say? Your security and your privacy online. Steve Gibson is here, GRC.com. He's our Explainer in Chief. Hi, Steve.

Steve Gibson: Hey, Leo. Great to be with you again as we close in on the end of our 11th year.

Leo: Yikes.

Steve: Episode 557 and a Q&A. We had lots of news this week. We're going to talk about - we're taking a look at Let's Encrypt's continuing certificate issuance, amazing progress. Something known now as the "Snowden effect" on the rate of encryption in general. What the cost was, both in dollars and public perception, to unlock what turned out to be a relatively empty iPhone. There's a clever Windows AppLocker bypass. And the way this works is just so cool. So I wanted to talk about that. That was buzzing a few days ago.

Opera announced that they have a built-in VPN in their browser. Unfortunately, it's not true. So we'll talk about that.

Leo: Ooh, I know, wow.

Steve: TeslaCrypt, the bad ransomware, has continued to evolve. We even have something that was predictable, which is DDoS extortionists that have actually no botnet because they've never actually DDoSed anybody, but they're still making a lot of money, just because everyone's so worried about it now.

Leo: The threat is stronger than the execution.

Steve: Yeah. The U.S. has launched its first-ever "cyberbomb" at ISIS. And what's odd is that they're talking about it because they're actually waging a little bit of a public relations campaign at the same time. So we'll cover that. I wanted to mention something that I forgot to talk about, about DNSSEC. I have a public service reminder for our listeners. And then we've got great questions and talking points from our massive audience. So a great podcast.

Leo: Nice. As usual, lots to say, lots to do. All right, Steve. Let's get the news here.

Steve: So Let's Encrypt continues to grow. And the growth is not linear. It's exponential. Meaning that you can't fit a straight line to this curve because it keeps curving up faster. So the rate of its growth is increasing, in addition to the absolute number of issued certificates. They said, the EFF said last Thursday that they had issued their two millionth domain certificate on last...

Leo: Wow.

Steve: You know, a little over, or a little less than a week ago, five days ago, eight weeks after finishing its first millionth. So they did their second million in less than eight weeks, whereas it took them a few months, I think they began at the beginning of December 2015. So the rate at which - the length of time between successive millions is shrinking as this thing is really catching fire. And they reminded us that, since single certificates can and typically do often cover many websites, Let's Encrypt is probably newly protecting many more millions than just two. And the EFF also noted that nearly all of the new certificates are protecting domains that were not previously HTTPS. So this represents just a sweeping increase in encryption. And it's interesting because we have some comments made by - I'm going to get this right this time - Comey. We've got both Clapper and Comey in our news this week.

Leo: As usual.

Steve: Yes, as usual, and not in a good way. So because it was Comey whose - no, I'm not sure. I've got to wait till we get to this in the notes because I don't want to get them wrong again. But so anyway, Let's Encrypt is a success. And we talked about how - what's the big blogging site? I'm just - I'm drawing a blank now.

Leo: WordPress.

Steve: WordPress, how WordPress has adopted Let's Encrypt and is now providing...

Leo: It's really cool because you just get HTTPS automatically, for free.

Steve: Yeah, I mean, you know, my two blogs, GRC.blog dot - wait, is it GRC dot - no, blog.grc.com and steve.grc.com, those are CNAME records in GRC's DNS that redirect people to the blog pages. And when I went there after reading that WordPress was all HTTPS, sure enough, my blogs are now HTTPS. So you can go https://steve.grc.com, and it works. Although the certificate is interesting to look at because, as I recall, mine, the certificate that is protecting me is shared with I didn't even count how many other domains. So WordPress is minimizing the number of certificates they issue by just cramming as many - they're called SAN, it's the SAN field, the Subject Alternative Name field is just full of other domains. So it's useful for basically removing plaintext from the 'Net.

And we'll be talking about that theme a couple times this hour because - or in this podcast because that's sort of the way security is turning out to be - we talked about this a little bit last week, how this notion that, yeah, the math is perfect, but it's impossible in the real world, or impractical in the real world, to obtain the level of actual security that the math provides because of all the difference between the math, which is ivory tower, and the implementation, which is, you know, who made the chips, who burned the ROMs, who made the hardware, who wrote the OS, who created the apps. I mean, there are just so many other things that can go wrong, each of which has the potential for compromising security, down from the absolutism of the math.

Leo: You know what I would love to see? I wonder if they're going to do this. I would love to see Let's Encrypt offer signing certificates for email and stuff. What that would do is empower encrypted email much more easily for people because they'd just download the certificate, and most email clients will handle it, and...

Steve: There have - I have seen some notes about sort of off - I don't know what the term is. Off the standard uses of Let's Encrypt. For example - go ahead.

Leo: I mean, I guess, I mean, it's a certificate. But you can't - it's not the kind you would use for email. Or is it? I mean, couldn't they do the same thing for email that they do for HTTPS?

Steve: You absolutely could. For example, GRC's email is using our DigiCert certificate and is offering TLS connections on the alternative ports, not the old...

Leo: I mean having a certificate on your computer when you sign your email so you can have signing and encryption in your email client. I don't mean for the email server. I mean encrypted client-side encryption, a client-side service.

Steve: Yeah, yeah. These are tied to domains, though, so...

Leo: Yeah, you can't, yeah, you have no - that's what I'm saying is you'd have to do a different kind of cert.

Steve: Right.

Leo: The p7s or the S/MIME.

Steve: Right. But you're right, it certainly makes sense for someone now to extend this notion to create personal certificates.

So it was Clapper who yesterday morning, in a breakfast sponsored by the Christian Science Monitor, and he's of course the Director of National Intelligence (DNI), he stated that what he called "Snowden's surveillance leaks" have...

Leo: Ugh.

Steve: Yeah, have prompted, he called it, a "massively accelerated push to improve encryption, with the result that today the world is seven years ahead of where it would otherwise be if 'Snowden' [in quotes] had never happened." And I just...

Leo: What a nonsense quote. I don't even...

Steve: Isn't that interesting? I thought it was interesting that, you know, I mean, this is bureaucracy, and this is the level at which he operates where they have some sense for the rate at which encryption is being adopted. You know there must be, like, people with degrees generating papers.

Leo: And there's a graph somewhere, yeah.

Steve: Yeah, exactly, generating papers, talking about the number of encrypted devices because this, you know, the notion of encryption is clearly a threat to the degree that it removes plaintext from the 'Net because, when we first started talking about Snowden, when in fact my hypothesis was that there were taps that were installed, which we later found out to be the architecture that was in use, they were happily siphoning up a bunch, I mean, like everything that went by. And at the time a lot of it was still in the clear. When we talked about Firesheep, way back then, it was something which you could install in Firefox which would allow you to obtain all of the plaintext of people operating around you on unencrypted WiFi. And it was just - it was the way the world was then.

Well, it's changed dramatically since then. And there's no question that the Snowden, the Snowden revelations were a wakeup call to an industry that, you know, we were moving forward with encryption. But, for example, Let's Encrypt, with its exponential, you know, way more than two million domains now encrypted, it's a reaction, probably, to this. So I think he's certainly right. But I just thought it was a - I got a kick out of seven years.

Leo: Yes.

Steve: And Clapper said, "From our standpoint, it's not a good thing." Then...

Leo: See, I feel like that's propaganda because I feel like it's very clear they have better ways to surveil us than they've ever - we're seven years ahead of where they would have been in surveillance, thanks to the Internet of Things, the widespread use of open WiFi, and on and on and on. They've got massively good means. I mean, how did they solve crimes before we had smartphones?

Steve: Now, I'm not disagreeing that there is - for example, we've argued that metadata, and many people are now agreeing, that metadata is arguably almost more useful than the data that the metadata is describing. That is, the content can be completely unknown, yet it's the who-called-who-when linkages which is still very difficult to obscure, and incredibly valuable from an intelligence standpoint.

Leo: And I feel like there's - I think there's some disinforma- and of course we don't trust Clapper anyway. He's a known liar.

Steve: No, no.

Leo: But there's some misinformation.

Steve: He's the famous, you know, tell where he was scratching his head, lying directly to the Senate Committee.

Leo: Here's what I wonder about. He knows, surely he knows, Comey knows they actually have many more resources and much better Intel about people than ever before. That's obviously true. And so why do they keep banging this drum? What is it they really want? Why is it that they don't want encryption? It's more than just tracking down terrorists, I feel. It's got to be more than this at this point. They have lots of means now.

Steve: I just think they can cry, and they can pull the national security card, and they can pull the terrorists, and we hear about the child pornographers and, you know, and the - how can it possibly be that criminals can have communications that we can't see? And so they're, you know...

Leo: That's a red herring. You know, whenever they raise child pornography, you should know that there's something going on behind the scenes; right?

Steve: Right.

Leo: But I think I general it's a red herring, that they want you to think it's all about terrorism. What is it really about? Why do they care so much whether we can encrypt our email, or I can have an encrypted chat with you, or...

Steve: I think it's just that they would rather we didn't. I think...

Leo: They want everything. They want it all.

Steve: I think that for the last 30 years most of what was happening on the Internet was in the clear. Email was in the clear. We briefly went to a secure connection to pass our login credentials to Amazon or Facebook or wherever. And then, because encryption was expensive in terms of overhead, the standard operating procedure was drop you back to HTTP. And so, I mean, there was - it was a treasure trove of absolute plaintext that they could do keyword searches in, and they had their little probes installed all over the Internet, and they...

Leo: So there was a magical golden age of surveillance, briefly, when we first got on the Internet, and we were putting everything out there unencrypted.

Steve: And everybody was happy that it just worked.

Leo: Prior to that, they had...

Steve: We were all just happy that it worked at all.

Leo: Prior to that they had less information than they have even in this encryption era. So they said, oh, we had a golden age for a year or two. We want that back.

Steve: Oh, no, no, for decades. Decades.

Leo: Well, the Internet really wasn't widespread use till the mid-'90s. So two decades.

Steve: Okay.

Leo: Two decades, that's all. So they had a gold- and by the way, in those golden years, did they eliminate terrorism? No. Arguably, it was worse then than it is now.

Steve: Well, and the terrorists are using this technology to huge advantage.

Leo: But before they didn't have the Internet, so they would write notes to each other or something; right? So...

Steve: Well, and as I said last week, absolute security is an illusion. It is unobtainable. And if you actually want a conversation not to be overheard, you meet on a park bench, you know, where you can see everything around you, and you whisper to each other.

Leo: Right, which is what you did until recently.

Steve: Right.

Leo: So we're, I mean, you could say there's no way we're taking a step backward. If anything, we've taken - made it easier for law enforcement.

Steve: Well, and as it turns out, this leads me to the next note of this week, and that is - I titled this "Our taxpayer dollars hard at work." And this follows the news that the FBI reportedly paid a hacker $1.3 million to unlock the San Bernardino shooter's iPhone that had been - that was the one that he'd been given by the county.

Leo: And 8,000 college graduates, computer science graduates, decided they were going to into the hacking business. Payday.

Steve: Well, and the way - it was funny because the way - now, this is Comey. The way he said this was bizarre. So this was last Wednesday. Speaking at the Aspen Security Forum in London, our FBI Director James Comey provided a roundabout hint about the price it paid, "it" the FBI, to an unnamed outside party for the hacking solution which, as we know, followed Apple's refusal to help the agency bypass the iPhone security mechanisms.

He said, when he was asked how much the FBI paid for what they called a zero-day flaw that allows the FBI to break into Farook's iPhone, Comey replied, quote: "A lot. More than I will make in the remainder of this job, which is seven years and four months for sure." And so people, like, okay. Well, public records indicate that Comey earned $183,000 last year. And without a raise or bonus, he will make $1.34 million through the remainder of his job. And so that's where we've come up with this $1.3 million figure was from this bizarre comment, "More than I'll make for the remainder of my employment as FBI director." So it's like, uh, okay.

The problem is that, in losing, essentially losing both of these court battles, the argument can be made that the FBI is way worse off today than they were before. The Verge had an interesting story, Russell Brandom wrote it, and I'm just going to paraphrase from it. But as we know, on February 16th, the FBI took Apple to court over the Farook iPhone, and Apple refused to comply. Meanwhile, a similar phone unlocking order was already being argued in New York.

Well, essentially those two cases plunged Apple into a legal crisis because the company faced the possibility that a ruling might undo a lot of their security work. Well, here we are now, two months later. The fighting is over. And the FBI's hoped-for legal solutions were both defeated. It's always been clear to observers that the FBI hoped to establish legal precedence with these cases, both which failed. As we just noted, they ended up dropping the pursuit, in the case of Farook's phone, after paying a hacker $1.3 million, apparently.

And now of course there's the question of are they going to make what they learned available to Apple. And now, I just saw today that Apple is - or the FBI is saying that, well, we really don't understand it well enough for there being anything for us to give Apple. It's like, okay. Observers believe they just want to keep it to themselves, even though we have been told that it doesn't work, it's inapplicable to anything newer than the 5c that was the phone that the county had given to Farook. Moreover, after losing the fight in New York, the judgment came down against them. The FBI promised to appeal that negative decision.

Then late last Friday, which is where you drop news you just sort of don't want anyone to notice - it's famous, you know. Friday afternoon or evening is the news dump where you just don't want it to be in the cycle. It's the reverse of Monday. And so late last Friday they said that they had, quote, "found the passcode" for this phone that was at issue, for which there had been a negative judgment against them which they promised to appeal, so they've dropped the appeal.

So now, with the New York case closed, the government is no longer attempting to use the courts to force Apple to break its own security. As we know, there are plenty of other iPhones prosecutors would like to unlock, but not a single other active case. So essentially the FBI retreated in both of these instances, did not get the outcomes from a legal standpoint that they were hoping. And it's left them with, essentially, with bad judgments that now stand and show no indication of being appealed. So it was not a good couple months for law enforcement. Yikes.

Also in the news, a very clever AppLocker bypass was discovered. There was a security researcher, Casey Smith in Colorado, who had the problem of wanting to get a reverse shell on a machine that was locked down with AppLocker. As we know, AppLocker was a technology that was introduced with Windows 7 which essentially is a white- and blacklisting system that allows, typically in an enterprise environment, allows systems to only run approved-of software. And so this guy was trying to get something to run on a system that was locked down with AppLocker, essentially a whitelisting system that would only run permitted software. And so, faced with the problem, he found a solution, which is really interesting.

Leo: It was kind of clever, actually. And it's scaring the pants off me. We use AppLocker here.

Steve: Yeah. And so it turns out there is a tool that is in the Windows System32 directory called "regsvr32" and "regsvr64." It is a means of registering OLE controls, the Object Linking and Embedding controls, and also COM controls, DLLs, ActiveX things, with the operating system. So, and it's something that's for - sometimes installing software requires you to register these controls. And it's sort of supposed to be done automatically. It's not something users typically do. But sometimes when, like, stuff breaks, part of the advice is run this regsvr, and they'll give you this magic incantation command line. And you first unregister the thing, and then you reregister it. And it just sort of rehooks it into the system again.

Well, it turns out that what was not known is that the command line which you pass it in a /i: argument, can be a URL. And it's just like, what? Who knew that? Somehow Casey figured this out. And what's troublesome is that regsvr is trusted by the system. It's signed. And it has been given by default firewall permission. So Microsoft knew that regsvr, their regsvr utility - and maybe Microsoft uses this, and no one was really aware of it because it could be just done sort of by scripting internally, to go out on the Internet and obtain scripts to run.

And so Casey did this. He set up a script on a remote server. And it can either be JavaScript or VBScript. And as we know, JavaScript and VBScript, especially now that it's able to invoke PowerShell stuff, I mean, you could do anything with this. And so this is an element in Windows which is trusted by the system, has firewall permissions by default, understands proxying by default, so it's able to get out through corporate proxies also. So basically it cuts right through all security, and it bypasses AppLocker completely.

Leo: Amazing.

Steve: So using this with essentially a simple command line, Casey was able to essentially invoke external scripts to run applications of his choice, even though AppLocker did not permit them to run, because essentially he was getting this trusted regsvr to do it on his behalf.

Leo: It seems like Windows has gotten so complicated.

Steve: Yes.

Leo: That you just can't keep track of everything that's there.

Steve: That's exactly right. And as we know, nothing is the enemy of security more than complexity. And exactly as you say, Leo, it is just - it's so complicated, there's just ways to do this. And so from a theoretical standpoint, the idea that he had a problem, and he decided to solve it, it's like, oh, how many other hackers have had this same problem and have solved it, but haven't told us? You know, he told us. And so the only reason we know about this is that he's a good guy, and he put up a proof of concept. And he said, oh, by the way, this works. And so presumably Microsoft will do something there, probably in, you know, next month on Patch Tuesday there'll be something to fix this. Who knows what? Now...

Leo: Might be hard to fix because a lot of things may depend on this.

Steve: I was just going to say that, exactly. If in fact they are using the URL-ness of this, and one thinks they probably are because they've given it explicit firewall permissions, it may break stuff to close things down. In fact, the only workaround that anyone has at the moment, and this is what people are recommending if you're concerned, would be to remove firewall permissions, both from regsvr32.exe and regsvr64.exe, in order to prevent it from being able to reach out of a network and grab potentially extremely powerful scripts to run without anyone's permission on a system.

It looks like a local concern. This is not something where it's, for example, opening ports and servicing requests from the outside. So it would be a local bypass of AppLocker. But that's what AppLocker is meant to prevent is local programs that are unauthorized from running. So this is definitely creating a breach where an enterprise or other system is using AppLocker to lock it down. This says, eh, no, we're going to run a program anyway.

Leo: Yeah. And we spend a lot of money for AppLocker. I mean, and it isn't so much to keep our employees from doing bad things. It's just we want to keep these machines kind of - these are our editing machines, you know - stable and not insecure. It's not about employees.

Steve: Oh, Leo, and having ransom cryptoware...

Leo: Exactly.

Steve: ...rifle through your network, that would not be a good day...

Leo: Not good.

Steve: ...at TWiT, no.

Leo: Yeah.

Steve: No. Even with backups of everything, you still have downtime that would shut down production significantly.

So Opera posted an item on a blog that generated a huge flurry of excitement last week. They wrote: "Today we want to share with you another big thing that you will first see in the developer channel for Opera for computers." And I guess they mean Opera for computers as opposed to Opera for mobile or other platforms because, you know, they have been trying to push Opera out into other environments, you know, embedded uses and so forth.

They said: "We are the first major browser maker to integrate an unlimited and free VPN, or virtual private network. Now, you don't have to download VPN extensions or pay for VPN subscriptions to access blocked websites and to shield your browsing when on public WiFi."

So that generated, as I said, a lot of interest. The problem is that it isn't a VPN. It's actually a - maybe we should call it a browser super proxy service. So, and we've talked about Opera proxying for years. This is one of the tricks that they've used on their mobile platform in order to offer their service and to minimize bandwidth consumption. They would proxy connections and, for example, re-render large images to make them smaller in order to optimize the performance of their mobile Opera.

So the argument is that what this really is, is an encrypted browser proxy. It does hide your IP address because Opera will replace the IP address with the IP of one of their proxy endpoints. And I'm calling it a "proxy endpoint" because it isn't actually a VPN. The problem is that a virtual private network has a universally agreed-upon definition. And that is that it is a tunnel around network bandwidth that inherently encrypts all network bandwidth. But this doesn't. What they've done is it's - what a traditional browser proxy does is proxy HTTP, that is, just HTTP proxy, meaning that other protocols like, for example, video, which wouldn't be HTTP and would get blocked by firewalls that are controlling what you have access to, they wouldn't be tunneled in a strict web proxy.

So what Opera has done is they have expanded the coverage of their proxy so that, for example, specifically, web videos are proxied. And so they say that they unblock firewalls and websites. Many schools and workplaces block video streaming sites, social networks, and other services. By using what they are saying is a VPN, they say you can access your favorite content, no matter where you are. And of course you do get the geographical jumping aspect of it because your public IP is one of their - one of Opera's endpoints where your traffic emerges. And they note that public WiFi security, when you're surfing the web on public WiFi, they say intruders can easily sniff data. And that's of course true if it's not secured. Then they say using a VPN you can improve the security of your personal information.

The problem is it doesn't even capture everything, even everything your browser could do. For example, the whole WebRTC protocol is not in this VPN of theirs, which is not a VPN, it's really a proxy. So the problem is they've done more than proxying. Unfortunately, they have overstated what they've done. And they were forced to respond to the industry that was taking exception to this. And their head engineer, Krystian Kolondra, he attempted to clarify this and said: "In our case we are coming with a new term, a browser VPN. And our goal is that all the network activity from the browser is actually routed via our secure proxy, unlike the usual proxies that only route the web traffic. So it's different than a system-wide VPN, but it's also different than a proxy, thus a browser VPN."

And then he says: "Currently, WebRTC and plugins are still not routed that way. But we're very open about this. We've just released this as a developer preview and planning to fix this in the coming updates." So even by their subsequent acknowledgment, they're not a VPN. They are capturing additional queries beyond HTTP and routing them through their proxy. So anyway, I wanted to just sort of clarify for everyone who was excited that this is, you know, not a free VPN. It doesn't mean that, you know, that I think it's clear that email and anything you did not in the browser would not receive the benefit of this.

And unfortunately, even everything you do in the browser does not receive the benefit of this. Only a few more things, some additional things, like - and they haven't made it really clear. But, for example, viewing web videos. Apparently they're capturing that so that it wouldn't be clear to anyone who was explicitly blocking those that that was being done. And you do get encryption. So, I mean, so it's not without its purpose. It's just not - it's stretching it to call it a VPN. And, you know, so I salute it, but it's not clear that it's going to move a lot of people.

Leo: Would it be hard to do a VPN? I mean, you'd have to pay for it, obviously.

Steve: Maybe they're going to migrate in that direction. Maybe they'll...

Leo: But that's the first step, right, because now you're proxying traffic.

Steve: Right.

Leo: You can proxy - it wouldn't be that hard.

Steve: But to be a VPN, it would have to be something outside the browser.

Leo: Ah, right. I get it.

Steve: That's the key.

Leo: I get it.

Steve: Yeah. So what would be nice, and I hope they'll do this, would be, for example, to capture WebRTC and plugins so that, as they're saying, right now they're doing more than just proxying HTTP, but there's a lot they're still not doing. What would be clean would be to at least capture everything the browser does. And, for example, it's not clear that they're even capturing DNS. They're probably not. So that anyone monitoring DNS would still be seeing all the various sites that your browser was asking for IPs for. So it's just sort of messy. It'd be nice if they had total encapsulation of everything their browser was doing. That would be cool. Right now it's like, eh, sort of a work in progress. And we'll sort of keep our eye on it to see where they go. But to be a real...

Leo: So it's better than nothing.

Steve: Yes.

Leo: It's just not a VPN.

Steve: Right, right.

Leo: Oh, that's all right. And they may be misrepresenting it slightly.

Steve: Yeah. And unfortunately they used the term VPN and got everybody excited because, wow, wouldn't that be cool?

Leo: Right, yeah.

Steve: But, yeah, not so much. So unfortunately there's a new version of TeslaCrypt out. And it's like version 4.1a. So now our crypto ransomware has version numbers. The worrisome thing about it is that it's got stronger obfuscation strategies. It's getting much better about evading antivirus. It's got anti-reverse engineering technology in it, much stronger stealth. And whereas we were seeing some targeting, you know, spearphishing, apparently, of high-value targets, like we've talked about various hospitals that have been crippled with this, now what's happening is the various security companies that watch the Internet are seeing TeslaCrypt as part of high-volume spam flooding campaigns.

So, you know, one of the things that I do, and something I would recommend for any of our listeners that are positioned within an organization, when I hear things like "Cryptoware is now in high-volume spam campaigns," I just send a little email to Greg and Sue, just to sort of remind them. Because, you know, this is happening. This is really bad. You know, yes, we can recover. But it's really better if it doesn't happen to you. So just don't open attachments. You know, just continue, I mean, they're really good. They're not getting themselves infected. But a little reinforcement is, I think, useful to remind them.

Oh, and the other thing is that the ask from the high-volume campaigns is lower. So they're asking for a smaller piece of a bitcoin. But what's been noted is, unfortunately, they're making it up in volume, so...

Leo: Oh, lord.

Steve: It's like, oh.

Leo: It's like a real business or something. Wow.

Steve: Yeah. Yeah. Boy. Meanwhile, you'll get a kick out of this, Leo. On the next page I've got a copy of the email which is being sent. Okay. So this was a Cloudflare blog posting. What happened starting last month, in March, is that Cloudflare's customers - and of course Cloudflare is providing DDoS protection for sites that are having this problem and needing to put themselves behind a large pipe proxy, essentially. They began forwarding to Cloudflare's management email that they've been receiving, telling them that unless they paid money to the Armada Collective, which is a well-known DDoSing gang, that their site would be blasted off the Internet, and they would not be allowed back.

So, let's see. Reading from this email, it says: "Forward this email to whoever is important in your company and can make decision. We are Armada Collective." And then there's a link. And I think the link is to a Google search. And what's clever about...

Leo: Yeah, "lmgtfy" stands for Let Me Google That For You.

Steve: Ah, perfect.

Leo: And so this is the snarky response you give to somebody who asks a painfully obvious question they could have discovered the answer to on Google in moments. You send them the link, lmgtfy.com, with the query attached.

Steve: Right.

Leo: When they click it, it pulls it to a Google page with a prefilled query.

Steve: Right. So...

Leo: And we do that in the chatroom a lot. That's why I know.

Steve: So what's clever about this is it leverages the reputation, the DDoSing reputation, of the Armada Collective to substantiate their existence and their claim that they'll...

Leo: It's just saying, just Google us.

Steve: Right, exactly. You can see how real we are. So they say: "Your network will be DDoSed starting" - and then they fill in a date - "if you don't pay protection fee, 10 bitcoins," then the bitcoin address. And so, what, bitcoins are now on the order of $400, so that's $4,000 that they're asking for.

Leo: Wow.

Steve: Yeah. Then they say, "If you don't pay by [date], attack will start. Your service going down permanently. Price to stop will increase to 20 bitcoins and will go up 10 bitcoins for every day of attack." They say: "This is not a joke. Our attacks are extremely powerful, sometimes over one terabit per second. And we pass Cloudflare and other remote protections, so no cheap protection will help. Prevent it all with just 10 bitcoins," and then they provide the bitcoin address.

Leo: But if you act today...

Steve: Right. "Do not reply. We will not read. Pay, and we will know it's you, AND YOU WILL NEVER HEAR FROM US AGAIN," it says in all caps. "Bitcoin is anonymous. Nobody will ever know you cooperated."

Leo: Wow. I can see that this would scare some people, if you...

Steve: Oh, lord, yes.

Leo: Yeah.

Steve: And, I mean, a lot of companies are going to get this and think, I mean, especially companies that are like, $4,000? Uh, ow. But they're hearing the stories about sites being blasted off the Internet all the time. And now they get this demand letter from a legitimate DDoSer with a reputation, the Armada Collective.

Now, there are just a few problems with this. First of all, they use the same bitcoin address for every one of these demand letters, and the same 10 bitcoins amount. Bitcoin is anonymous. So in fact they cannot determine who paid them.

Leo: Right. They will have no idea.

Steve: They have no idea. Despite that fact, the fact that these are blind demands for payment that they have no way of knowing, the Chainalysis group that watches the blockchain have found more than $100,000 paid...

Leo: Oh, man.

Steve: ...to that bitcoin address.

Leo: Wow.

Steve: So these guys are making money.

Leo: Holy cow.

Steve: At $4,000 a pop. Oh, and Cloudflare, of course, that broke the news of this, also talked to their competitors and found their fellow DDoS preventers' customers were also receiving this. And not a single instance of an actual attack.

Leo: Right.

Steve: So there is no teeth behind these threats. They can't know whether anyone paid them or not because it's the same bitcoin address. So they're just making money. Oh, and this was in less than eight weeks. So this is $100,000 in less than eight weeks.

Leo: So what do you suggest? Wait till somebody actually does a demonstration of their DDoS capability before you hand over the money? Just say, like, hey, if you're real, just take me down for a minute, would you?

Steve: There isn't a good solution.

Leo: There's no way.

Steve: I mean, exactly as you suggest, Leo, the way for a legitimate attacker to function is to take the company down for a period of time, or actually to send email saying...

Leo: I will take you down, yeah.

Steve: ...we're going to demonstrate our ability, yes. It has to be done...

Leo: Anybody who's ever seen a Bond movie knows the evil villain has to do a demonstration that he has the nuclear weapon before he can actually blackmail you.

Steve: Right.

Leo: So you've got to blow up an island first.

Steve: Right. And he has to notify you he's going to so that that solves the problem of someone saying, "Oh, I'm the one who did that," even if they weren't. So only by notifying you ahead of time, and then doing it, can they establish causality. And then they say, okay, you've seen what we can do. If you don't want to live your life that way, pay up.

Leo: And by the way, somebody in the chatroom's a little confused because they said, well, no, DDoS attacks are real. We're not saying that there aren't DDoS attacks.

Steve: Oh, you remember "GRC Is Down."

Leo: Some people know about this.

Steve: "GRC Is Down" was the title of this podcast a few months back, yes.

Leo: But these are unsubstantiated ransom requests.

Steve: This, unfortunately, I mean, and the - I mean, it causes, I don't want to say it causes a problem for the DDoS industry.

Leo: It kind of does because credibility, their credibility's shot now.

Steve: Right.

Leo: I'm not paying you. You're just phony. I love it.

Steve: And in fact, in Cloudflare's blog post, because they are so highly ranked in Google, they are hoping that this explanation of this fake demand will rank highly in Google so that that link will fail. That is, it won't only be legitimate instances of this group, but a very public expose on the fact that these demand letters are just bogus.

Leo: If you want people to believe you have a Death Star, you've got to destroy Alderaan first, or you just don't have the credibility.

Steve: Yeah, so a horrible ripple is felt.

Leo: Thousands of voices shouting out.

Steve: Yes. Yes. So the U.S. was sort of surprisingly public. And David Sanger, who's a well-known reporter for The New York Times covered this in a story that was titled "U.S. Cyberattacks Target ISIS in a New Line of Combat." David wrote: "The goal of the new campaign is to disrupt the ability of the Islamic State to spread its message, attract new adherents, circulate orders from commanders, and carry out day-to-day functions like paying its fighters. A benefit of the administration's exceedingly rare public discussion of the campaign, officials said, is to rattle the Islamic State's commanders, who have begun to realize that sophisticated hacking efforts are manipulating their data." I mean, and I'm thinking, thank goodness we're doing that. "Potential recruits may also be deterred if they come to worry about the security of their communications with the militant group.

"Defense Secretary Ashton Carter" - who's oft quoted - "is among those who have publicly discussed the new mission, but only in broad terms, and this month the Deputy Secretary of Defense, Robert O. Work, was more colorful in describing the effort." This is the line that caught my attention. He said: "'We're dropping cyberbombs,' Mr. Work said. 'We have never done that before.'" So apparently we are cyberbombing ISIS.

And then David wraps this up, saying: "The fact that the administration is beginning to talk about its use of the new weapons is a dramatic change. As recently as four years ago it would not publicly admit to developing offensive cyberweapons or confirm its role in any attacks on computer networks. That's partly because cyberattacks inside another nation raise major questions over invasion of sovereignty. But in the case of the Islamic State, officials say a decision was made that a bit of boasting might degrade the enemy's trust in its own communications, jumbling and even deterring some actions." So, okay. I'm glad that they're, you know, that we're using our cyber technology to that end.

I did want to mention Hover again, my new - and I'm very happy with them - registrar because, after talking about the catastrophe of SMTP Simple Transport Security (STS) last week, and how what we really needed was DNSSEC, I spent a little time digging around, looking at what it would take for GRC to sign its DNS records. And it turns out that among the things it takes is registrar support.

Leo: Mm-hmm.

Steve: That is, support from your registrar, because the registrar has to provide, I think it's DS records they're called. Maybe it's domain signing. I just dug in enough to get a sense for what it would take. But it's crucial that your registrar be able to take records that typically you provide to them and include that in your official domain registry entry. Well, Hover can. Network Solutions, and I was stunned by this, cannot. I mean, they are the venerable registrar of the Internet. I'm with them because I registered GRC.com like around the same time Microsoft.com was first registered. You know, we were - this was the beginning of the Internet, and they were where you registered.

Leo: Yeah, I was with them at first, Network Solutions, yeah.

Steve: Yeah. Everybody was. What I found interesting was that, in looking at charts and tables that exist on the Internet of which registrars do offer this, the ones that were the favorites of our listeners all do support DNSSEC.

Leo: Oh, interesting. So that would be Google, Hover - yeah.

Steve: Yes. Even Namecheap, for example.

Leo: Namecheap, yeah.

Steve: You know, the hip registrars do support DNSSEC. But many still don't. So one other thing to consider at some point, if DNSSEC is going to - when it starts to happen, when we start having things that are really valuable to protect. Signing is still a pain. It's, I mean, it's like, I looked into it, and it's like, okay, well, nothing I have really needs it, so I'm going to wait until something does because, oh, it really does - it's a mess. But one of the things you need is registrar support. So I said, ooh, does mine? My new one? And the answer is yes.

Leo: Yeah.

Steve: So right now I still have - I bought a bunch of years. I'm not sure when GRC expires at Network Solutions. But, boy, I will be moving it to Hover because today, at this moment, I could not, if I wanted to, have DNSSEC support on GRC.com because my registrar, the registrar for GRC.com, doesn't offer it. They just figure they don't need to.

Leo: So the registrar has to have it, not the nameserver.

Steve: Nameserver, too. So...

Leo: Yeah, nameserver as well. But you can't just use somebody else's nameserver. You have to have the registrar support it.

Steve: Yes. There needs to be records added to, essentially, to the domain root. You know, so somewhere there is a, you know, there is GRC is a record in the dotcom servers. And it's my registrar that provides me with that linkage with the GRC record in the dotcom servers. So those records need to have the DNSSEC, I think they're the DS records, added to them. And so your registrar needs to be able to do that. And Network Solutions can't.

Leo: Good.

Steve: I can't get away from them fast enough. Oh, I'm so happy with Hover.

Leo: December 2017, somebody says.

Steve: Ah, is when GRC...

Leo: GRC expires, yeah.

Steve: Yeah. I wanted to give a quick public service reminder to our listeners. A number of people in the last couple weeks, probably because of the success of Never10, have been setting up new instances of Windows 7 and saying that Windows Update never does anything.

Leo: Oh, that's not good.

Steve: Well, and I've talked about this. And so I wanted to remind everyone because people - so for all of our listeners who, in the future, have an occasion to set up a new Windows 7 machine, the problem is that even the Windows 7 SP1 image, you know, the ISO that typically you start with, it is old now compared to Windows Update. So when you install a brand new Windows 7 with SP1 built into it, which is about 175 updates behind in the first round - it takes, like, five rounds of updates of updates of updates of updates before you're done. But it reaches out with its - with the Windows Update client that it had when it was SP1, when it was brand new.

And unfortunately the protocol has changed. The protocol or the domain, something has changed. I haven't bothered to dig into it because I don't care. But the point is it doesn't work. So the first thing you have to do after installing a brand new Windows 7 is update

Windows Update. And you have to do it manually because it can't do it itself.

Leo: Great.

Steve: Because it's too old.

Leo: That's lame.

Steve: It is so lame. It is so lame that, like, I mean, and Windows 7 is still supported, you know, like through 2020. So it's just wrong that they changed Windows Update and broke the Windows Update for a version of their operating system that is still supported. So I created a bit.ly link for this, and it's wupup, Windows Update Update. And so it's bit.ly/wupup, all lowercase.

Leo: Wupup.

Steve: That will take you to the Update Windows Update page on Microsoft. You download that EXE, run that, and it's a standalone installer that will bring Windows Update up to current so that then it's able to go find the 170-some updates.

Leo: But what's weird is that you're downloading an ISO from Microsoft for Windows 7. Oh, maybe they're installing it from a DVD that they had lying around. If you get the Windows 7 ISO from Microsoft, it should have an updated updater.

Steve: No.

Leo: No?

Steve: It's the image from then.

Leo: Oh, can't fix the image.

Steve: I know. I know.

Leo: I'm increasingly coming around to your point of view on all of this. I don't use Windows, period. I'm just so - it's just - I feel like it's just - it's too old. It's just become crufty. And I'm much happier with Linux. And I just bought a new Windows PC.

Steve: Oh, and things like OLE and ActiveX and COM+, I mean...

Leo: It's all just kind of hanging out in there.

Steve: We've been through so many bad stages where...

Leo: Yeah. It's like a soup with old clams. It's like they don't want to refresh the ingredients. They just want to keep all the old ingredients lying around, just in case.

Steve: Yeah, now, to their credit, they did, with Edge, they dropped IE, and they started over. So, you know, and Edge is doing well from a secure standpoint.

Leo: They didn't really drop IE. It still comes, IE still comes with Windows 10.

Steve: That's true, it's there. You're right.

Leo: They did not drop it. They can't. That's the problem. I mean, it's not completely their fault.

Steve: Right, because it breaks too many things.

Leo: Yeah. They have to preserve downward compatibility. Legacy is everything in Microsoft. But what are you going to do?

Steve: It would be nice, it would be nice if they could just start over. It's like Mozilla needs to start over with Firefox.

Leo: Yeah.

Steve: Some of this stuff just gets too old, and it's, well, and in fact we've even been seeing this with OpenSSL. It's so old, I mean, it is the absolute reference code, which is like a mixed blessing because, you know, we talked about how Amazon has created a vastly smaller and simpler build, you know, their own TLS, which does everything they need, and it's, what was it, like 5% the size? And it's not - it's because it isn't the kitchen sink. It doesn't have all this other crazy stuff in it which is just all the legacy that OpenSSL has. But it works.

Leo: There really is no reason now not to use Linux, except for you because you're writing Windows software. But everybody else, Linux has just - the more I use it, it's really mature now. It's not old because you can...

Steve: And I listen to you guys...

Leo: ...[crosstalk] that just has the features you want. You don't - you are in charge of what legacy's there.

Steve: Right. And I listen to you guys on MacBreak Weekly, talking about how sometimes just an iPad is all you need.

Leo: Yeah.

Steve: And also sometimes just a Chromebook is all you need.

Leo: Chromebook is a good choice. For most people, a tablet or a Chromebook is really all they need. A general purpose operating system is not necessary. That's old days. In the old days, you didn't have a choice.

Steve: Yup.

Leo: But we've come a long way. We do have a choice.

Steve: And I think it is telling that Intel is making noises now about...

Leo: Wow, they're moving away.

Steve: ...moving, yes, moving away, looking at other...

Leo: I like my desktops. You know what I'm hoping at this point, that AMD kind of survives, first of all - that would be a nice start - and can kind of create some solid kind of privacy-focused chips for people who want to roll their own. You know, it seems like there's an opening there. We've really moved into an appliance, computing appliance world.

Steve: And I think what's happened is we've seen many stages. There was a day about, ooh, 25 years ago, when you could charge for a mouse. That is, you could charge for a GUI where you had a mouse and a cursor that, like, moved on the screen. And so we had GEM, and we had Windows. And, you know, that was like a big deal. Then that became commodity, so that everybody had that. There was no more - there was no value there.

And what we're seeing now is the operating system is now a commodity. Everybody knows how to make them. There's a bunch of them that are free. They're open source. They're build your own. They're, you know, what desktop do you want? You know? And so we're sort of, in the same way that we're sort of in the post-GUI era, I mean, we have them, but, you know, you can't get any money for that anymore. That's just part of the ground. And now operating systems are, too.

Leo: Yeah.

Steve: I've been having some discussion over in the spinrite.dev group, like next generation, and sort of like thinking about how I'll do SpinRite 7. And the idea is that, you know, because I'm a Windows developer, and I know this environment so well, and I'm so comfortable here, that SpinRite 7 might be a bunch of custom kernel drivers to give me the super low-level access that I need to the hardware, and then a feature-full Windows application that talks to the custom drivers. So anybody with Windows who purchases SpinRite 7 would be able to run SpinRite without leaving Windows; would be able to perform recovery on their drive, even the one they're using, assuming that it boots; and do all kinds of SpinRite things on attached storage of any kind without leaving their operating system.

And the ReactOS, which is coming along very nicely, is 100% Windows API-compatible and driver-compatible. Which means I could take the entire identical set of work, SpinRite kernel drivers and a SpinRite Windows app, and host them on the ReactOS for everyone who was using Linux or Mac...

Leo: You use FreeDOS right now; right?

Steve: Right.

Leo: This would replace FreeDOS?

Steve: Right. And so for, like, for the next major revision of SpinRite, you would be able to boot SpinRite with the ReactOS if you didn't have Windows. Or if your Windows...

Leo: And that would run on an ARM chip, too; right?

Steve: Uh-huh. And that's the other thing, is that...

Leo: Oh, interesting.

Steve: Is that I would make it platform independent and bring it - I would finally give up, you know, in the rewrite, lift it away from assembler, rewrite it in C so that it would be cross-platform and cross-architecture, too.

Leo: Very interesting.

Steve: So anyway, just some discussions that we've been having about how I might do this. I've got one more interesting piece of news. I got a long DM from a neat, I want to call him a kid. I don't know how old he is. Just sort of felt like a neat developer kid. I'm sorry if I'm insulting you. His handle is Inphektion.

Leo: Inphektion.

Steve: Inphektion. Yeah, there you go, good. Inphektion.

Leo: That's definitely a kid, by the way. I don't know anybody over 25 that would use that as a handle.

Steve: Right. So he says: "Hey Steve, nice chatting with you, ha ha. Wondering if you could help get the word out about the easiest way for a layperson" - and it's not really a layperson, but, you know, he wrote that - "to set up their own OpenVPN server. I consider this similar to helping people, just as Let's Encrypt has helped lower the bar for website owners to offer their sites over TLS. This allows anyone who is able to boot a Raspberry Pi to install and manage OpenVPN. I call it PiVPN. Installing it is as simple as entering: 'curl install.pivpn.io | bash' into the command prompt. That's it. I have a site up with more information at pivpn.io."

Leo: This is a great idea.

Steve: It is.

Leo: Use your Raspberry Pi, a $35 Raspberry Pi as an OpenVPN server.

Steve: Yes, yes. I loved it because what this lets our listeners do is you take a Raspberry Pi, and you just plug it into your router. After setting it up, you plug it into your router, and it's an OpenVPN server. So what that would mean is that, wherever you were out and about, as long as you knew the IP of your home, and of course you could use dynamic DNS, DynDNS, to do that, you could VPN into your home network. So that would allow you then to get out to the Internet, so you'd be VPNing away from where you are, and your IP would be your home's IP. And of course you'd also be able to get onto your home network with access to all of your home resources.

So what's so cool about this is, you know, curl, and then install.pivpn.io. That pulls what you need and pipes it through bash that does all of the work for you. So it's a script that installs OpenVPN server and configures it and sets it up. And you can even manage the server because you have - he says you have add, list, and remove, et cetera, commands for managing the client certificates. So he says he'd greatly appreciate me getting the word out, and I have. And I think this is a cool idea. So I salute you, Inphektion. PiVPN.io. I think I - I haven't tried it myself.

Leo: I'll try it. I'll try it. I'm going to try it.

Steve: Looks like a cool solution.

Leo: Yeah. I'm going to try it. Now, the Raspberry Pi has an ethernet port, and you could put WiFi. Because you'd need dual - wouldn't you need dual ethernet to do a VPN?

Steve: You really don't. We think of it that way, but there's no reason that it could not route from the outside and back to the [crosstalk].

Leo: [Crosstalk] loop. So it goes through and comes back out. Okay.

Steve: Yes.

Leo: So a single ethernet would be adequate.

Steve: It could be set up that way. I don't know how he's done it. But...

Leo: This is a trend which I'm loving. And Let's Encrypt is another good example of this, of people taking the effort to write scripts that automate these processes that you could do by hand. I mean, they're cookbook processes. But it's, as you mentioned when you talked about setting up an OpenVPN server, it's nontrivial.

Steve: It's what drove me to consider CryptoLink.

Leo: Right.

Steve: Was, you know, I got mine running. I use one. But, oh, boy, it's not for the faint...

Leo: Yeah. So, and I'm seeing, by the way, more and more of this. And I love it. And there are tools, there's tools like Jenkins designs to build these automated - Jenkins is an automated build server. But for developers it automates this process that used to be very tedious and manual. And the reason I think of Jenkins is because there's a great little program to build a Raspberry Pi, or actually could run on anything, a Minecraft server. And you just run this, it's a Java program, but it basically is a long script that does all - that grabs stuff from where it needs and assembles it and puts it together. It runs for, like, 20 minutes. And at the end you get a JAR file...

Steve: Nice. Nice.

Leo: ...that is the whole thing. And it's so nice. I think this is a great - this is, if you're not a programmer, but you're an accomplished user that knows how to install stuff...

Steve: Exactly. It's sort of a - it's like a perfect middleware thing where, you know, you're able to pull all the pieces together and create value.

Leo: Exactly. I'll try this. I see no reason not to, despite the name Inphektion, I see no reason not to try it. And I'll let you know how it works. The nice thing is...

Steve: Cool.

Leo: ...it's Raspberry Pi. Worst-case scenario, you format the MicroSD card and start over.

Steve: Yeah.

Leo: Yeah.

Steve: Yeah, cool. Very cool. So we all know that one of my pet peeves is non-zero-based Y axes on graphs. And I loved this. Somebody found this and tweeted it to me, and I said, oh, that's the Picture of the Week. Well, it got bumped down into Miscellany by the exponential growth of Let's Encrypt. But I just love this. The caption is: "Is truncating the Y-axis misleading?" And this shows a chart where essentially 1% says no, and 99% say yes. But because the Y-axis has been truncated so that the zero is essentially 98, it looks like it's an even split.

Leo: Equal. It's a perfect example.

Steve: Between yes and no.

Leo: Perfect example.

Steve: Yeah, loved it.

Leo: Yes, it's awesome.

Steve: And then going through the mailbag, I did find a note from a Rob Peel. And I'm hesitant to pronounce this Australian city name because I mangled, what was it I mangled...

Leo: Yeah, Canberra. Canberra. Canberra. Canberera.

Steve: ...Canberra last week.

Leo: Canberra.

Steve: So what do you think? Geelong, you think it's Geelong?

Leo: That one you got me. Geelong? Geelong? Is it a hard or a soft "G"? Is it "jif" or "gif"?

Steve: Yeah.

Leo: Geelong.

Steve: And then we heard - someone said it was "yif" now. I've heard that used.

Leo: Yeah, "yif," I'm saying "yif."

Steve: Okay.

Leo: Because that way you get out of the whole battle.

Steve: That's right. We're just going to go - we're going to take the road less traveled, the third branch.

Leo: It's "Yeelong."

Steve: So he says - so anyway, his note was in the mailbag, and it was about my switching to BSD or Linux and the suggestion for a podcast, a different, a new podcast that we would do, Leo, to follow my journey into that territory. And so I just thought, okay, well, no.

Leo: Just what we need.

Steve: I don't think so. But, he said, "P.S.: I purchased SpinRite a few years ago, and when a friend's XP machine was failing to boot recently, I had a chance to give it a go. I pointed SpinRite at the hard drive and came back once it had finished. It hadn't appeared to have found any problems." This is a popular refrain we've heard before. So he says, "So I was beginning to think it could just be Windows rotting away as it seems to do when it has users installing all those search bars. Anyway, I restarted the machine, and she booted straight up without any errors. Magic," he says.

And then, separately, I thought you'd get a kick out of this, Leo, as would our listeners. Someone who's a longtime SpinRite user has been collecting what we call the "detailed technical log" screens, which is a graphic representation of what SpinRite found on the drive. And I've got four of those screens in the show notes that he provided. The first one is just a really bad day.

Leo: Oh, yeah, man.

Steve: It's just, yikes.

Leo: Lots of red.

Steve: Lots of red unrecoverables, where SpinRite, despite everything it tried, it would have ended up approximating the data in the sector. And as we know, that's not as good as a perfect recovery. But sometimes, you know, sometimes it just means that a few bits ended up it couldn't figure out, but all of the other 4,096 bits it could, or all but, I mean, there's a total of 4,096, so a few it lost; but the rest, the balance of them it was able to get. And if, many times, even an executable will run if something like - if a small part of it is broken. So definitely worth doing if you're in recovery mode. So that's one of the reasons SpinRite wins as much. But the other three are interesting because they evidence the physical nature of data destruction.

Leo: Oh, look at that.

Steve: Yes.

Leo: So it's like slices. It's like slashes of green.

Steve: Well, think about it. The disks all have a periodicity to them. That is, there are surfaces, and there are platters. And so, for example, if a surface died, then...

Leo: It would look like this; right? It would be kind of stripes.

Steve: Yes. And in fact I think this represents a problem that, that second image, a problem with one whole surface. It looks to me...

Leo: So just so people understand who are watching this, red means an unrepairable bad sector. Green means a repairable bad sector. So those are bad sectors, those stripes.

Steve: Right. Well, so, and notice that the unrecoverable ones were at the beginning.

Leo: Yeah.

Steve: Then we had a whole region where SpinRite was able to repair the problem. And then notice how at the bottom they kind of taper off, that is, they're not as wide because whatever it was that went bad, it was sort of fading out there toward the end. And then at the very end of the drive there was no problem. So it's really interesting that you see the cyclical or the per-surface nature, the physical nature of the problem.

Leo: Geometry shines through, yeah.

Steve: Yeah.

Leo: How about this one?

Steve: And then the third one is the same kind of...

Leo: Perfectly evenly scattered dots.

Steve: Yup. So there is a - there was, like, the head bounced on the drive, or scraped across the surface or something. So spaced out in equal distances across..

Leo: What is the X and Y? Is it - do you start at the center and move out from top to bottom?

Steve: Correct. So the upper left is the beginning of the drive.

Leo: Zero sector.

Steve: And we know that that's the inner cylinder. So drives always start in the inside and move to the outside. I'm sorry, no, disks do that. I think drives typically start on the outside, on the outermost cylinder, and then move inwards. And so the upper left is the beginning of the data, and the lower right is the end of the data.

Leo: So on a spinning hard drive, this is probably the outside. Because that's the fastest part of it is the outside; right?

Steve: Correct. Correct.

Leo: It starts, it uses this first because that's the best part to use.

Steve: Exactly. You get the highest data transfer rate.

Leo: Right, right, okay. And then this one?

Steve: And then the last one is fewer, but still the same sort of periodicity showing that there was something physically where there was a problem. I just thought those were kind of cool.

Leo: Really neat. Somebody in the chatroom said, "There is a limit on how much you should do SpinRite." He said, "I have a friend who used SpinRite 33 times in a month on the same drive because it kept coming up with errors."

Steve: Oh.

Leo: There is a point at which you discard the drive; right? I mean, there are - it is also the fact that sometimes the error is not like a hard or a permanent error. Relocating the data and marking that sector bad will keep a drive going. It's like back to, you know, continue to use it.

Steve: Correct.

Leo: But there is a, what, how many times should somebody run SpinRite on a single drive before giving up?

Steve: I guess it's sort of a function of your situation.

Leo: If it happens again, like you fix it, and you're using it, and then you have another problem, and you run SpinRite again, and there's more bad sectors, that would be enough for me to say, hey.

Steve: Yes. I would say it is absolutely the case that, if a drive insists on failing, nothing SpinRite can do can prevent that from happening.

Leo: Right.

Steve: That is, you know, it is - SpinRite, think of it as providing you a big, a much larger gray zone than you ever had before, between the drive is all happy and the drive is dead. SpinRite, like, instead of that just being white and black, now there's this gray zone that allows you some leeway in, like, saying no, no, no, no, I really need this back.

And so, you know, run SpinRite on it, and it'll say okay. You were in the gray zone, but you weren't that deep in. So we'll give you your data back. But it's like, yeah, take that as a hint that, you know...

Leo: Yeah. Get your data off and move on.

Steve: ...maybe you don't want to stay in, you don't want to get any deeper in the gray zone.

Leo: [Singing] Riding in the danger zone. I want to ask you a question. Then we've got 10 questions from our audience.

Steve: Yup.

Leo: But just a quick question about just - I'm getting a new Thunderbolt 3 enclosure. These new Thunderbolt 3 enclosures. 40Gbps, I mean, just...

Steve: Oh, wow.

Leo: I'm so excited. And then I'm putting into it SSDs, the top-of-the-line Samsung EVO 850s.

Steve: Nice.

Leo: Yup. And it's a two-drive enclosure with hardware RAID. You could do zero or one, or you can span, or you can just say, hey, there's two drives in there. Is it nutty for me to do RAID 0, the striped RAID? It gives me a 2TB drive that's fast; right? Although is it faster on an SSD?

Steve: Yes. Well, it depends upon the RAID controller.

Leo: Okay.

Steve: Striping is supposed to be faster.

Leo: It interleaves rights, goes right here, right here, right here. But that's to compensate for seek time. And there's no seek time on an SSD.

Steve: No, but so the problem is the interface you've got is faster than the drives.

Leo: Right.

Steve: And so that's what we're...

Leo: Oh. I get it.

Steve: Yeah.

Leo: I get it. Okay. So we're getting a faster throughout by interleaving the drives.

Steve: By pulling from both drives at the same time.

Leo: Oh, at the same time.

Steve: Yes, yes.

Leo: So I would want to use RAID 0 for maximum throughput.

Steve: Yup.

Leo: Because the drives can't saturate the bus. The bus is way faster than [crosstalk]

Steve: Correct. If the RAID controller - the question is, is the RAID controller good enough to pull from both, or to cache and then write to both?

Leo: I'll have to do some tests and see. I don't want it redundant. I don't care about that. I want speed.

Steve: Yeah. Yeah. Well, and...

Leo: And 40Gb.

Steve: With the size of the stuff you guys are throwing around there, I mean, you know, the overhead of producing the shows just, I mean, I'm hearing you talking about all the video compression stuff.

Leo: Oh, can you imagine? Our render times are huge.

Steve: Yeah.

Leo: That is, unfortunately, the biggest issue for us, getting these shows out. We'd love to turn around and show the show - and people all the time say, why does it take so long? We'd love to give you a show the minute it's done. But you've got to render the thing. So video, it's all about video. Video takes forever.

Steve: Yeah. When I'm sending the audio to Elaine, the time of the evening that I send it is a function of how long the podcast was.

Leo: Yes.

Steve: Because as this podcast is longer, we end up with the rendering time expanding. And so your guys just aren't able to get it posted any faster.

Leo: Yeah, you know, and there's actually two parts to that, two functions to that because what we do is we - and of course, if we didn't have to do video, none of this would be a problem. If it were all audio, everything'd be a lot faster. And so for things like TNT, the daily news show, we do just push the audio the minute it's done, so you at least can audio as quickly as possible.

Steve: Yeah.

Leo: But not only is it rendering, but upload. These are big files.

Steve: Yeah.

Leo: So we get it, and the new place will have better bandwidth for...

Steve: Ooh, nice.

Leo: ...half the cost, yeah.

Steve: Nice.

Leo: We have a number of fiber choices and gigabit - we have Gigabit from Sonic.net and...

Steve: Oh.

Leo: It's a little pricey. I can't - I don't think we get the Gigabit. We'd love it, though. All right, Steve. Q&A time. You ready?

Steve: Yeah.

Leo: We've got about half an hour, but I think we can burn through a few of these. Let's start with Redding. In the U.K., Neil Warwick writes: Isn't it time to drop Firefox? On a couple of recent podcasts you've mentioned some things that make me wonder, should I stop using Firefox and switch to Chrome? The last thing you mentioned, the namespace bug in Firefox, that was last week, was a little worrying - I agree - especially since I use the LastPass plugin, and I worry another malicious plugin could steal my data. Also, given that no one at Pwn2Own even bother with Firefox because it's so easy to attack makes me think maybe I should be looking for something else. My preference would be Chrome. No reason to stick with any particular browser, but I'd be interested in your view. You're still a Firefox user, aren't you?

Steve: I am. But I empathize with Neil's position. To be frank, I'm on Firefox because I love the add-ins.

Leo: It's the plugins that you're hooked on.

Steve: Yeah. Although now, you know, Chrome - when Chrome was new, it didn't have comparable plugins.

Leo: Oh, it's got amazing [crosstalk], yeah.

Steve: Now it's pretty much caught up. I really love the side tabs. And there is a Chrome plugin that offers that. But for me, the biggest problem is RAM use because I'm stuck in a 32-bit OS still. And as we know, Windows XP only gives you three of the 4GB of RAM. And I just - I can't afford to have lots of tabs in Chrome. The security modeled in Chrome is a multiprocess model where they use the OS-enforced process isolation in order to create inter-tab security. That's a good model, except that it's expensive in terms of memory. It's the reason Chrome tends to consume memory. As you open lots of tabs, those are each at least one process, sometimes several processes. So, and it consumes memory.

Now, when I switch to Big Mama, my 64GB of RAM machine, memory will no longer be a problem. And I guess we have to sort of see what happens with Firefox. I'll be a holdout, probably, just because - but I am going to end up running, figuring out how to put this thing in a VM. There is no way that, as soon as I can afford to, my browser does not go in some kind of a true high-security container. And the only real way to do that is to stick it in its own VM. Browsers need to be in virtual machines so that they cannot, they do not have access, uncontrolled access, to the underlying operating system.

But for most people, I kind of have to agree with Neil. I think that, until Mozilla revamps Firefox, and I hope they can, just in the same way that Windows is getting old, and we said earlier that Firefox is showing its age, because the architecture has been dragged forward now for so many years that at some point you just have to say, okay, we need to start over. And I love Firefox. But I have to say most people, I think, probably better served with Chrome.

Leo: Except Windows XP users. Right?

Steve: Who like tabs.

Leo: Well, but also Chrome is not being updated for XP now. So Firefox is it. That's your last best safe browser.

Steve: Right.

Leo: Unfortunately. Mike Hodos - Hodor! - in Raleigh, North Carolina wonders about the difference between a hardware firewall - well, you know, this is a good - I can't wait to hear your answer. This is a question that comes up a lot, especially on the radio show. What's the difference between a hardware firewall and a NAT router? And are there benefits to the hardware firewall in addition to a properly configured NAT router?

Steve: So I agree, this is a great question. And I see it all the time, too. So I was sort of trying to figure out how we got where we are. And it's mostly a function of history. That is, in the beginning, we didn't have consumer NAT routers because there just wasn't a need for multiple IPs. We typically had computers with modems that were dialing a modem pool remotely to get us on the Internet.

Meanwhile, corporations were getting themselves on the Internet, and their networks also were small, and they were being given blocks of IPs, which they needed, but they needed to protect them. So this was before NAT, but still a need for packet filtering. And so a hardware appliance was created to be inserted at the perimeter of an Intranet in order to control access to the Internet. And that was a hardware firewall. It was an appliance. It was something that was typically very expensive.

But corporations said, oh, you need a hardware - you need a firewall to protect your network. And of course movies all then had firewalls, and hackers were breaching firewalls. And so it was a thing. And it was sort of a - it was a device that had a role in the beginning. And, as we've seen, nothing ever goes away on the Internet. You know, it's why I'm hoping that SMTP STS never happens because, as I said last week, kludges never die. And but so what's happened is you could - there are still hardware firewalls. Not for any reason except sort of there were hardware firewalls back when we really did need them.

And now we have NAT routers because fewer IPs are being given to people who need many more. And the classic example is the residence, where we've got one IP being shared among now all of our light bulbs and other things in our home. So the distinction between a hardware firewall and a NAT router has really been lost. We've got terminology - hardware firewall and NAT router - which has survived the loss of difference between them. There really is no difference. NAT routers have additional firewall capabilities where you're able to punch through the NAT in order to create a DMZ. That's an old-school sort of firewall term. And firewalls all offer NAT as a feature of them. So there really is no difference anymore.

And then for a while remember there was the whole stateful packet inspection, where it was like, ooh, an SPI NAT router. Well, yeah, but all NATs are stateful because that's what NAT is, is stateful. So what we have is have sort of redundant terms - hardware firewall, NAT router, no difference. Just different terms now for what has essentially become merged into the same single thing.

Leo: There must, I mean, we spend - okay. There's definitely a difference in firewalls. I mean, we use heavy-duty enterprise-grade firewalls. And so there's definitely some additional...

Steve: No.

Leo: No?

Steve: No.

Leo: Because these are like $10,000. And I would like to not buy them.

Steve: Well, okay. So are they doing...

Leo: These are security devices.

Steve: ...antivirus?

Leo: They do other stuff, right.

Steve: Yeah. So, see, that's not a firewall. That's a - yes.

Leo: Security device.

Steve: That's a network security appliance.

Leo: Okay, okay, yeah.

Steve: So it's a firewall plus.

Leo: Like the Astaro. That's what the Astaro was.

Steve: Right.

Leo: Yeah, okay.

Steve: And it's doing way more than just being a firewall.

Leo: Yeah, we're using Astaros now, but they're close to their end of life, and we have to decide in the new building what we're going to get, I guess, yeah.

Steve: Yes.

Leo: Okay. Because otherwise I'm just going to say go out and get some Linksys routers, and we're good. Don't laugh. I don't want to be DDoSed. Dontrell in Georgia, he's being driven crazy with spam email, Steve. Guys, I was introduced to your podcasts through a course I'm taking - wow, that's neat.

Steve: Yeah.

Leo: And I want to know how I could stop - by the way, we hear from a lot of people, lot of college professors and others. People use this in their curriculum. I'm really - that's wonderful. I wanted to know how I could stop all the unwanted emails I get. I've tried the usual way of unsubscribing. Oh, no. But I think when I unsubscribe I start getting more unwanted emails from another unknown source. Yes, that's right. Sorry if I'm off subject of what you guys usually cover, but I'm looking for any advice. This is a good subject, too, another great question.

Steve: It's another great one.

Leo: You talk about what you do, but I'm going to talk about what I do because I have a solution, as well.

Steve: Okay. So I do two things. And I just sort of wanted to share this. Now, I have the advantage of running my own email server, so I can do some things that are less easy. But there are ways to do them, for example, with Gmail. So I do two things. One is I change my email address annually. That is, my email address incorporates the current year number. And what's cool about that...

Leo: Steve, don't give away your algorithm.

Steve: What's cool about that...

Leo: I thought that was secret.

Steve: Yeah. It's important.

Leo: You're more open than you used to be. Now that you do these Twitter DMs and all this stuff, you don't mind a little bit of...

Steve: Yeah. So the algorithm does include my email address. I mean, I'm sorry, the email address includes the current year. What's cool about that is that, if somebody has my email address from the prior year and sends me something, and it bounces, then they can look at it and go, oh, I'll bet I know what it is now. And so they just update the current year after January, and it goes through.

What this has taught me, though, what I discovered is the reason this was worth divulging my algorithm. I don't know why, but spam takes time to find you. And something as simple as changing your email address loses spam. That is, it's just gone. And you might think that, oh, it's going to find you again within a week or two. No. It takes, I can attest to this, years, multiple years. Because what I typically do is I forward the old addresses into the new address, just so that I'm not losing something I might care about. And so, you know, I'm getting some spam from 2011, for example. And I know that because it's got the 2011 number in the email address. But I'm not getting spam from 2012, 2013, 2014, 2015.

Leo: Oh, that's interesting.

Steve: It really is. So whatever the mechanism is, there is a long lead time. And so just what I've learned from experience is just changing your email address periodically sheds it for quite a while. And if you do it in some way so that people you care about could figure out where you've gone, then you lose the bad guys, you lose the automation, but not the humans.

The other thing I do is for - and this is where I use my own server. I'm able to easily create aliases. So, for example, DigiCert, I don't use that annually expiring email for DigiCert because I have to go change DigiCert and everybody else. So Amazon and DigiCert and PayPal and, you know, the relationships that I have that are long-lived and that are trustworthy, I give them a static email address for them. And that's an alias that then forwards to whatever my current email address is. So then I just quickly update the aliases in the server after January 1st, and everything keeps flowing through.

So those are the two things I do. And I mentioned the alias because, as we've talked about, it is possible to create aliases on Gmail accounts in order to create essentially individual accounts and get some sense, you know, get additional control over email.

Leo: You could do it with a plus sign. You do your name plus, and it ignores anything after the plus sign. So I use Gmail. I find Gmail is plenty for spam filtering. So what I do...

Steve: So just running email through Gmail.

Leo: I just - I have - so of course I don't use a Gmail address. I use my own address that I have with a registrar, with Hover. And then you send me email at that address. It just - Hover has an MX record that says go, you know, send - no, I don't want it. I don't have a server. Send it to Gmail. Gmail does, I think, very good collaborative spam filtering. So that's kind of the best kind. Computers are okay.

Steve: Right.

Leo: But they're not great. So the collaborative filtering means that, when somebody else in Gmail says that's spam and marks it as spam, and enough people give it that signal, Gmail will say, oh, you know what, this is a spam. And even though I didn't know it because my computer wasn't that smart, I'm not going to give this to anybody else. So that's great.

Steve: So you wouldn't even know. You wouldn't even know you were being DDoS extorted.

Leo: Yeah, no, I don't - yes, perfect example. Because people would mark that as spam. So that, I have basically a sewage treatment system. You know, sewage treatment is a multiple-stage system. So that's my primary treatment. Then...

Steve: Water comes out the other end.

Leo: Yeah. Eventually we're going to have pure email. The next thing I do is I send it to my IMAP provider. So they use Cyrus, which is a really excellent IMAP server. That's FastMail. So it goes from Gmail with my public address to a private address that no one knows at FastMail. That way only mail from Gmail is going to get to FastMail.

Steve: Yup.

Leo: Which is kind of what I want. I want it to be that primary treatment for everything. FastMail runs something called Spam Assassin, which is a more old-school but very, I think very effective, if properly configured, antispam filter, as well. That'll catch any strays that go through. But then filtering, the final stage, the tertiary stage is my own custom filters. And I'm looking for stuff, first of all, addressed to me directly. But other things I look for, and this might help our correspondent, is if the word "unsubscribe" appears in the email body, now I know that's a mailing list. So I just put those all in a separate mailing list folder, so they never get in my Leo inbox; right?

And then I have - one of the things that FastMail does is it has my address book, which I upload and keep synched. If somebody's in my address book, they're presumed to be a friend. They go to a friend folder because that's never a spammer. I also have a VIP list, and those are a handful, like my mom, that are - those get - that immediately goes to the VIP folder. And then the rest fall through to the Leo folder. And if it's not addressed directly to me, then there are lots of other places they might go. But those are much lower priority emails. They're mailing list emails or group emails, that kind of thing. And they're of less interest than something that's addressed directly to me. By doing that, and that alone, I find I am in pretty good shape. I rarely, rarely see spam. It's just - it just doesn't get down to that pure water level, you know.

Steve: Right. And I guess I would only say that the only difference, or the biggest difference, is I have zero filtering. So I never - so there's never any false positives.

Leo: Right.

Steve: I never - there's no danger of missing anything.

Leo: I don't see any on Gmail. False pos- but you're right, that's the risk of my system. The risk of your system is I get a lot of email, and I can't change my address every year. It's not - that's not practicable for me.

Steve: Right.

Leo: So you, you know, that system makes sense if you really don't want email, and only people who know your system can get through.

Steve: Right.

Leo: I can't do that. I have to have a public email address that anybody can email to.

Steve: Right.

Leo: So I have to use this. And there's one more additional thing I'd add, which is, if you do use Gmail, there's a plugin called Unroll.me that you can set up to automatically unsubscribe. So if you do get emails that are - that have an unsubscribe link, and that's almost all the emails that are from - they're ba- we call them bacon. They're not spam. You probably did sign up for them, or in some way indicated to somebody, yeah, it's okay to send me offers. But they're not something you want, either. So Unroll.me will give you some control over that. One way it can do it is a digest, with single email with all of them. Or it can actually unsubscribe you automatically. But to answer his specific point, that is kind of risky because a spammer wants to know if there's somebody at that address; right?

Steve: Well, and a perfect example of bacon is I mentioned that I had purchased some components from New Egg. Well, now I'm their best friend. And so they're sending me their daily deal constantly. And I, you know, I got that for a while. Then I thought, you know, no. And so I unsubscribed. And so it was a legitimate unsubscribe link from a legitimate retailer.

Leo: Right.

Steve: And I just said, nah, I don't need to know...

Leo: Periodically I'll do that.

Steve: ...that within the next 10 minutes I save 25% if I purchase this particular SSD that I don't particularly want.

Leo: What I find, though, is you can unsubscribe, and then a week later, two weeks later, everything starts up. You know, I mean, it is very hard to fight this. So automated systems seem to be the best. The nice thing about FastMail, very sophisticated filtering system that allows me to look at any part, you know, any X-header, any unusual - I can do - any part of that email I can parse with grep. And so you can get pretty - for a while, anything that came from China I was just dumping automatically. You know, there's stuff like that that you can get some pretty good rules in there. And rules will help you, too. That's kind of like that plus thing.

Steve: Let's do one more and then pick up the rest next week.

Leo: Okay. Sorry about that. I shouldn't be talking.

Steve: No, no, no. No, we've done a beautiful two-hour podcast, and we'll do another one next week.

Leo: Well, and it's Episode 1500 of TNT coming up in seven minutes, and we can't let that [crosstalk].

Steve: Nice.

Leo: Marissa in British Columbia, is that who you'd like to do next?

Steve: Yeah.

Leo: You know what's great? These questions that we've done are like the real fundamental questions we get all the time.

Steve: Yeah.

Leo: Nice to wipe them out. All right. This is the no-antivirus question: Steve and Leo, I've been listening to the show since the start of the year, and I'm hoping - so these are all people who are fairly new, I guess; you know? I'm hoping that I will become more knowledgeable in security, mostly by osmosis. Thank you so much for your interesting conversations and for sharing your infinite wisdom. Aw. Thank you.

My questions may show my true naivete, though: I was listening to a recent Security Now!, and Leo mentioned that you need not have an antivirus. What? I personally use Avira's free antivirus, and I like to scan to make sure that I have no intruders. Is there a better way to do this? Does this even protect me in the slightest? Can you recommend any episodes of Security Now! that could possibly teach me some more basics, or any other free - minimum-wage laborer here - educational tools. Thanks so much. I look forward to your podcast every week. Marissa.

Steve: So you and I are on the same page on this, which is that the AV which is now available for free - and I assume that Marissa is a Windows user. She didn't say. But Windows incorporates either, what, Windows Defender or Security...

Leo: It used to be called Security Essentials. And in Windows 10 it's just called Defender.

Steve: Right. And it's being updated. It's constantly updated. Microsoft has sort of slowly crept into this business so they wouldn't upset the existing AV industry that first formed around Windows. But at this point I just - I don't suggest anyone use a third-party AV. If something really gets - somehow passes that and gets in, I like - I just use Malwarebytes, free edition, run that to clean a system, and then remove it. But otherwise, I don't have anything running all the time.

Leo: I pretty much agree with that. The problem is that viruses spread so fast now that an antivirus probably isn't going to protect you.

Steve: Correct.

Leo: So in some ways that's a false sense of security. You get a free antivirus. You don't need one on a Mac, really. There's really not an issue on the Mac. And the other one I would say is there are a lot of companies trying to sell you antiviruses on mobile, on iOS and Android. And there's no reason in the world to use those. They can't do anything of value. And Google and Apple already do everything that can be done. In fact, Google will scan every app before you install it. And Microsoft won't even allow you to have an app that isn't scanned before. Doesn't keep stuff out of the store, but they have ways of killing it. And even if you download it, and it gets in the store, having a antivirus on iOS or Android is not going to prevent you from getting hurt.

Steve: Right.

Leo: So they're of limited utility. And they have some negative impacts. They slow your machine down. Sometimes they can keep you from doing things. A lot of the bugs that I hear about on the radio show, first question, I say, do you have security software running?

Steve: Well, and we also know that they've had some questionable practices, too, that they have installed security certificates in the root store, and they're looking at all of the security traffic coming in and out of your machine. Now, on one hand, it's like, well, yes, but that's local, and it's for your benefit. But if they're not careful, third parties can obtain the key and use that as a means of getting into your system. So it just - I don't think that, on balance, the benefit outweighs the collection of problems. And, for example, if you do have Windows, just use what's there.

And lastly, just to wrap up the question, Marissa, we do have a daunting number of previous podcasts, all of which are available. I don't have specific episodes of Security Now! that I would recommend for the basics. But we sort of did start at the beginning, in the beginning. And so if you've got time, you could go back to Episode 1 and learn about Honey Monkeys.

Leo: It's all still relevant.

Steve: And go forward. Yes, it is, it's surprisingly...

Leo: Alas.

Steve: ...useful. I did see in the mailbag somebody was referring to Episode 225, I think it was, and we were talking about how Apple was just expanding its input code from four digits to six. And he says, "It's still relevant."

Leo: Yeah. Isn't that interesting, yeah.

Steve: Yeah, even half the way back.

Leo: And Marissa, because you're a beginner at this, and we don't normally cover the really fundamental basics here, I'm going to point you to a website and a book that I interviewed the author. The book was scary. It was called "Future Crimes." But he's a computer security pro, and what he put together is an acronym called UPDATE.

And I'll run this by you, Steve, real quickly. But I think that you will agree with all but one. There's one that I kind of question. But these are kind of in order: Update frequently, number one. Passwords, he talks about making a good password, keeping track of your passwords, two-factor authentication. I think we'd agree.

Steve: Yup.

Leo: Download. This is what you've said. Only download software that you wanted, that you asked for.

Steve: You went looking for.

Leo: You went looking for. Be skeptical of free software, et cetera. Admin, which is don't run as the root superuser or admin user. This is the only one I - I don't dis- it's not bad, but he says turn off your computer because that reduces your attack surface.

Steve: No, I never do that.

Leo: That's silly.

Steve: Yup.

Leo: Because really the real problem is not while your computer is off, it's while you're using it. It's not when it's just sitting there. It's you that's the problem. And finally, Encrypt.

Steve: If we didn't have NAT routers, then I would say turn it off.

Leo: Maybe, yeah, right.

Steve: But, you know, there is no attack surface.

Leo: Right. And finally Encrypt. So it's not as good an acronym without the "T," UPDAE. But just remember you don't need to turn off the computer when you're not using it. But everything else, really, is actually very good, I think, solid advice. So he did a good job of that. It's FutureCrimes.com is the website. And then you just go to the resources or the...

Steve: How about instead of "T" for turn off your computers, train your family?

Leo: Train. Very good. UPDATE. Replace the "turn off" with "train." Because it is. It's about knowledge.

Steve: Yeah, because we are the weak link.

Leo: We are.

Steve: And so you want to explain, just as I said, like sending a little reminder to Sue and Greg, you know, I know everyone's good about not clicking on stuff in email, but really, really, really don't. And so you just want to, you know, you want to train your family and friends, you know, spread the knowledge that you get here.

Leo: Or "T" could be Trust No One. I don't know if that's...

Steve: That's good, too. Perfect.

Leo: Yeah, that's good, too, from Chickenhead21 in the chatroom. That's Marc Goodman. The book is "Future Crimes." I'm not necessarily recommending the book, but I do think - I mean, it's a good book, but it's not going to help you with security. It's mostly going to scare you. But the UPDATE acronym is good.

Steve: And I have to say, I mean, we have a daunting library of prior podcasts. But so many people say that they've, like, everything they know about security they got from the podcast.

Leo: Yeah. Well, that's true for me.

Steve: Or like it made it so easy to graduate with this or that degree and so forth. So there is, if you have time, there's - it's just dripping with, you know, information goodness.

Leo: Dripping with information goodness. That is our motto here at Security Now!. You'll find Steve at his website, GRC.com. That's where you get SpinRite, world's best hard drive recovery and maintenance utility, even for SSDs. GRC.com. But when you're there, there's so much free stuff that he gives away, including this show, and transcripts of the show, so you can read along as you listen. GRC.com. Questions can be left there, but he's also on the Twitter, @SGgrc, and accepts DMs from anyone, which is very - much more generous than I. Do not DM me.

Steve: Even if your name is Inphektion.

Leo: Inphektion. You're a brave man, I must say. We have audio and video of the show as well on our site, TWiT.tv/sn; on YouTube.com/twit; and wherever you get your podcasts, including those great third-party TWiT apps written by our friends, friends of the network, who have just done such a nice job on every platform. Look for the TWiT app and subscribe. You don't want to miss an episode. I still need to write a little script to download every episode. I should do that. All right. That'll be my task this week.

Steve: Yeah. You're having fun with scripts.

Leo: It's easy.

Steve: And command line.

Leo: It's not hard to do.

Steve: Yeah.

Leo: Thank you, Steve. We'll see you next week.

Steve: Okay, my friend, thanks.