Listener Feedback Q&A #44

Description: Steve and Leo discuss the week's major security events and discuss questions and comments from listeners of previous episodes. They tie up loose ends, explore a wide range of topics that are too small to fill their own episode, clarify any confusion from previous installments, and present real world 'application notes' for any of the security technologies and issues we have previously discussed.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-150.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-150-lq.mp3

INTRO: Netcasts you love, from people you trust. This is TWiT.

Leo Laporte: Bandwidth for Security Now! is provided by AOL Radio at AOL.com/podcasting.

This is Security Now! with Steve Gibson, Episode 150 for June 26, 2008: Listener Feedback #44. This show and the entire TWiT broadcast network is brought to you by donations from listeners like you. Thanks.

It's time for Security Now! Episode 150, our sesquicentennial episode. Steve Gibson, how are you today?

Steve Gibson: 150, I know, as I was writing that today I was thinking, yes, six to go, and we cross our three-year mark.

Leo: That's amazing. So today we're going to talk about security. In fact, we've got your questions and Steve's answers. We've got quite a few of them, a dozen great questions. But before we get to those, let's get an update on, first of all, any errata or anything you want to cover from last week's episode?

Steve: Yeah, a few things. I wanted to acknowledge all the people who wrote with the feedback that last week's audio sucked.

Leo: Yeah, apologies.

Steve: That's pretty much the only word for it. I think it was partly the microphone and partly - we're hoping it was the cable modem, meaning that you're switching your end to DSL, and of course I've got a pair of T1s. That ought to hopefully bring down any packet loss. We still have the possibility that it might be the fact that there's just video involved, and video competes [with] audio [for] bandwidth. And it might be winning. Anyway, we're going to try this one. I'm back to the Heil microphone that I've used for several years.

Leo: That makes a big difference. Yeah, that makes a huge difference, yeah.

Steve: Anyway, so I just wanted to acknowledge that lots of people wrote in to say, hey, Steve, just thought you should know, the audio last time was really bad. So we're working on it, and...

Leo: Yeah, I think mostly it was, I mean, everybody knows the audio, the microphone didn't sound as good, but it wasn't inaudible. It was I think the dropouts. And I'm still hearing [indiscernible] that, so I don't know what's going on.

Steve: Yeah, I'm hearing it from your end also coming back. Several people made the comment I thought was very astute, and that is that you have the Heil, and if I don't, then the difference in the quality of our audio makes it noticeable. That is, if...

Leo: No, I throw that out, you know why, because you're the only one with a Heil in the whole network.

Steve: And I also have been told, though, that I've always traditionally sounded better than any of the other netcasts.

Leo: And I'll be honest, I think it's your bandwidth more than anything else is probably the case. And I think we're still having bandwidth issues, and it kills me. I'm not sure why, but we'll figure it out. Skype is funny that way. You know, it'll go great for months, years, and then you'll have a bad day. And it's hard to predict. But we are on ostensibly the same exact setup we've used before with one addition, one slight change, as you said, is video. So maybe we'll just stop the video.

Steve: Well, yeah. And it's important to understand, too, that if we use less total bandwidth, then those packets have a greater chance of getting through than if we have just many, many more packets. So statistically, because as we've talked about many times the Internet delivers packets on a best-effort basis, as we crank our bandwidth up we're going to see larger packet loss.

Leo: Yeah, maybe that's it. Maybe just, you know, it's that Internet congestion thing you talked about a few episodes ago.

Steve: Yeah. So I wanted to mention that. And, oh, and there were some other people who were concerned that the audio portion of our podcast was going to be sacrificed at the altar of video. So I just wanted to say that that's not the case, that we recognize that the number of people listening to the audio far outweighs the number of people watching the video, and that I'm going to be conscious of that, and I won't start holding up charts and things so that the people who are on the audio channel feel disadvantaged in any way. So I wanted to make that clear also.

Leo: All right. Yeah, I mean, I think a number of the shows actually, because we're sending so much video now, a number of the shows have become very videocentric. The Giz Wiz, for instance, Dick's always holding up stuff, saying hey, take a look at this. It's kind of hard when you have a camera going. People kind of start paying attention to that. But it is, it's a much smaller audience.

Steve: And there actually were a couple people who are major TWiT people who wrote and said hey, you know, I've noticed that some of the other podcasts are sort of not really relying on the video, but exactly as you said with Dick, I mean, he's having fun with the fact that he's on camera. But people who are listening to audio can't see what he's holding up, so.

Leo: Right, right. Yeah, it's something I'm aware of. I'm going to have to think about it, and I don't know exactly what to do. On the other side of the equation is video has brought a lot more people to the party, including advertisers. So I'm not sure I want to dump the video, either. So we'll have to figure out a happy medium, shall we say.

Steve: Yes.

Leo: So what else is in the security news?

Steve: Two little blurbs on a recent event since last week. There's a weird Microsoft Word problem, believe it or not, with its parsing of bulleted lists. So that if you open a Word document that can be crafted to be malicious, it uses a buffer overrun in Word's display of bulleted lists to perform a remote code execution. As far as I know, this is not something that Microsoft has addressed yet, or patched. But we can hope that that's on the way.

Leo: Yeah.

Steve: And then lastly there is an unspecified remote code execution problem in all versions of Firefox through and including v3. There's no patch yet from the Mozilla folks. But I just wanted to let our Firefox-using listeners know that there is a known problem

which has been brought to the Mozilla people's attention that has not yet been fixed.

Leo: Yeah. There's also been a Mac trojan, did you see that?

Steve: No, I didn't hear about that.

Leo: Yeah. I'm not sure that - you know, the problem is once again that the people who report this are the people who make the antivirus software for the Macintosh. Or, you know, the security software for the Macintosh. So I'm always a little bit, you know, suspicious of the whole thing. But this for the first time is one that is in fact in the wild. It actually takes advantage of a vulnerability in the remote access client. And the fix right now, until Apple patches it, is to remove this ARD client from your system. You can actually just, you know, zip it up and stick it somewhere else so it won't run. And unless you're using remote access on the Mac, that's not going to be a problem.

Steve: Oh, yes yes yes, in fact I did hear about that. And someone posted a note asking how it could be that people who were running the Apple service were less vulnerable.

Leo: Yeah, so I don't know about that. That's interesting, yeah.

Steve: Well, what I heard was that, or when that was reported, it seemed to me that, if the trojan were trying to - technically the term is "bind." If it was trying to bind to that port, if the port is already open and bound to the application, then that would prevent the trojan from being able to do so.

Leo: Yeah, that's...

Steve: So it is that that would explain the fact that something, a service running makes you more secure technically than not having it running.

Leo: So that's exactly what happened. This ARD agent vulnerability was published. And then immediately somebody wrote a trojan to take advantage of it. And the companies that found out, first it was SecureMac and then Intego, both of whom make antivirus solutions for the Mac, talked about this. It does give you, it can give you complete access to the Mac, including this trojan can log keystrokes, take pictures with the built-in camera without your knowledge, take screenshots, turn on filesharing. So it is a big vulnerability. Generally will come in via iChat. So I guess the key is not to accept files from other people. It's a trojan. They have to send you an application for this to work, and you have to open it. So don't.

Steve: And I have to say, Leo, your audio has really improved.

Leo: Yeah. I think that the video was a mistake.

Steve: I think, well, what we can try to do, and we'll try this during our setup next week before we begin recording, is perhaps there's some way - and I'll screw around with it this end - for me to reduce my upstream bandwidth and not kick it into high-quality, high-bandwidth mode. Because after all, I mean, I'm sending 640x480 at 30fps. I mean, that's full broadcast-quality resolution. And the point is that no one - I'm sending it all to you, and then it's being reduced as it goes out through the redistribution and all that. So it's probably possible to lower the resolution and/or the frame rate, or maybe increase the compression without really having the user suffer at all, but also be much more bandwidth sparing.

Leo: Right, right. Yeah, we'll figure it out. I mean, as video is subordinate to audio, and this just shows, so by turning off the video, the audio is better, that's fine with me. We don't have to solve it.

Steve: Several tens of thousands of Security Now! listeners are breathing a sigh of relief.

Leo: Well, but the thing is, I like to see you. I mean, I think it's fun for people to see you, too. And...

Steve: We'll see if we can...

Leo: At some point somebody's going to say, okay, I want a list of all the books on the bookshelf behind Steve because he has a big, big bookshelf behind him and a lot of books on it, I might say.

Steve: A wall worth of books.

Leo: Hey, speaking of books, I just got Neal Stephenson's new book, and I'm really enjoying it, it's called "Anathem." It will be out in September. I got a reader's copy of it. And it's really...

Steve: Oh, very cool.

Leo: He wrote "Cryptonomicon," which we've talked about before, and is one of my favorite authors. So I'm reading a paper book, Steve.

Steve: Oh, my goodness.

Leo: It feels so old-fashioned.

Steve: Only because it hasn't yet been read into Audible, I'm sure.

Leo: Oh, yeah. In fact, I asked Audible about that, and they said, yeah, we know a lot of reviewers do listen to Audible for reviewing the books because it's more efficient for them to get the book read. And they said we should really talk to these publishers about when they send out a reader's copy we could also send out the Audible copy.

Steve: Yeah.

Leo: I guess they were - it takes a while to record these books. This is a big book. Take them a couple of months to record. But they start early.

Steve: Yeah, I don't think Neal has ever written a small book, has he?

Leo: No. His last book, "Quicksilver," if you go to the Science Fiction Museum in Seattle, they have the manuscript. He handwrote it with a fountain pen. And they have all the fountain pen cartridges, all the manuscript paper.

Steve: Oh, my goodness.

Leo: It's crazy. I don't even - it's nuts. But it sounds like his process.

Steve: Well, whatever works for him. I got a nice note from a listener in Hong Kong - oh, no no no, I'm sorry, in Korea, he's Korean, regarding Security Now! and his experiences on SpinRite. He says, "Dear Steve, how are you? I am Yong-Gu Bae." I guess that's how you - it's B-a-e, Bae?

Leo: Bae, yeah, Bae.

Steve: Yong-Gu Bae. He says, "I am a Korean living in China." Oh, living in China. "I live in northern part of China, so I live far away from Hong Kong Post Office." Of course referring to our mentioning that as a certificate authority on a number of occasions. And he says, "...far away from Hong Kong Post Office. However, it's a malware hot zone nonetheless. Since I am in export-import business, I travel a lot. And last year unfortunately I got my laptop bag stolen at Barcelona. So I lost my laptop, digital camera, external hard drive, and iPod. It was a big loss, and it took a fortune to replace all of them. So my European trip last year was the most expensive trip ever.

"More than three months ago I learned about Leo's TWiT podcasts, and I started to listen to Security Now!. I visited your website and downloaded all the episodes and PDF files. And I'm proud to tell you that I'm up-to-date with your podcast. While I was listening to your podcast I noticed that you were that Steve Gibson from GRC, where I copied Perfect Passwords for my routers about two years ago and downloaded SecurAble from about one year ago. I wish I listened to your podcast a little earlier so that I could have

prevented the robbery. Nowadays, thanks to you, I use TrueCrypt on my laptop to avoid another unfortunate incident, and use Hamachi to connect to my office PC. Since I was a computer science major, I have a lot of hard drives lying around. So while I was listening to your podcast I decided to buy SpinRite.

"I will be on a business trip to the U.S. from Thursday. But suddenly, two days ago, when I was working at the office" - and he says in parens, "(yeah, I work seven days a week these days)" - "my wife called me and told me our home PC isn't working. Sure enough, when I went home and turned on the PC, it was only showing Windows Vista logo with green dotted lines moving forever. So I put SpinRite to work using Level 4; and the next day, voila, the PC was working fine. I've used SpinRite in various hard disks that I own, both by CD booting and using VMware workstation." And he says, parens, "(I use 6.5 beta free edition and love it)." I noticed that to use VMware a lot, it's better to have a multicore with lots of RAMs. I use Vista x64, by the way. Thank you for reading my lengthy feedback, and thank Leo and you for a superior podcast. And best regards, Yong-Gu."

Leo: Thank you, Yong-Gu.

Steve: That was a neat note. I really appreciate...

Leo: Yeah, yeah, really cool. You ready for our first question of the day?

Steve: Let's go.

Leo: Let's go. Mark Madison in Pawlet, Vermont brings router malware to our attention. Router malware? Steve, the Washington Post's Brian Krebs - by the way, I read that column a lot, he's very good.

Steve: Yeah, Brian's a good guy.

Leo: Yeah. Brian Krebs reports that a new variant of the widespread Zlob trojan can change DNS settings in your router. So even if you reformat after an infection, as you and Leo recommend, you may still have a problem with your router. I know you've probably covered the basics already, but it might be worth mentioning this extra cleanup step after a bad infection. Reset your router. Thanks for the great show.

Steve: I thought that was really interesting. We've talked about the need to disable Universal Plug and Play, UPnP, in routers because of the virtual certainty that malware is going to begin to use that for router reconfiguration. It turns out that what this trojan, this Zlob trojan, this variant of it, apparently it's very widespread. Microsoft reports that they've cleaned off tens of millions of copies of it from people's machines using their constantly updating - is it Defender? I can't remember what they call it.

Leo: No, OneCare, Windows OneCare probably. Unless, well, Defender is spyware. OneCare is their antivirus.

Steve: Yeah, I think it's just Defender, you know, the one that everyone just gets, and it's always updating itself. Anyway, what this thing does is it has a huge list of default username and passwords for all the routers, in addition to hundreds of other likely passwords. So it's able to see what your gateway IP is. It then, behind the scenes, without you knowing it's doing it, it communicates with your router and knows what the default page is and tries to bring up that page and literally log into the router in the same way that you would, as someone doing local administration of the router.

And of course it turns out that a huge number of people have left their username and password unchanged. And I once confessed that I was among those people. That's since been changed. This is not for a mission-critical router, not inside my network. It's a completely disconnected router over on a cable modem that I just have here for visitors because I don't let anyone touch my network under any circumstances. But it was the case that I was thinking, oh, you know, no one can get in until they're in. And you have to be in in order to access the inside administration interface of the router. Well, it turns out that there is a way now, unfortunately, for if malware gets in, what it does is it is able to log into the router, change the DNS settings, which means that then - and this is the other interesting thing is that not only your machine, that is, the one that's already infected, but all the other machines that are using DHCP, the obtain-IP-address-automatically protocol from the router, every machine within your network will get the DNS from the router, which is reset to a malicious DNS server that then causes your browsers to go to the wrong servers whenever they're trying...

Leo: And why would they do that? It's not a denial of service, but they inject stuff in.

Steve: Yes. The idea is that you think you're going to PayPal.com, and you're going to their PayPal clone site.

Leo: Oh, interesting, interesting.

Steve: Not good.

Leo: And this one also pops up spyware. It does all sorts of interesting things. It posts spammy forum comments. I mean, this is a nasty little bug.

Steve: Oh, it's a busy nightmare, yes.

Leo: The chatroom is pointing out that it could also have been Microsoft's Malicious Software Removal Tool. They update that...

Steve: That's exactly what I was trying to remember. That is the name, yes.

Leo: So that actually does something. Because I get those updates all the time. It actually does something.

Steve: You know, Leo, that was a surprise to me, too, because I also - you don't think it's doing anything. I mean, it's certainly not in your face. But it's always, every single second Tuesday of the month, oh, we're going to update the Malicious Software Removal Tool. And I go, okay, fine. You know, and then it never tells me anything or seems to be doing anything. But on the other hand, you and I are being very careful about what we do with our machines. Clearly tens of millions of other people aren't, and they've got this Zlob trojan trucking around inside, messing up their networks.

Leo: I think probably Microsoft, I don't know, they don't want to give away a free antivirus, partly because they'd put themselves out of business with OneCare.

Steve: But yet at the same time they would love to do something about their horrible reputation from a security standpoint.

Leo: Right, right, right. I'm looking at their page on Microsoft. It looks for Blaster and Sasser and MyDoom, which are nasty ones. So I think in a way, if they have something that's looking for worms and trojans just to damp it down, I think that's a good thing.

Steve: Yeah.

Leo: Just damp down the spread of these things. Brian in Toronto works for Internet Service Providers using something called "transparent proxying." He says, Hi, Steve, I used to work for an ISP where proxy servers weren't just encouraged, but enforced. All port 80 traffic ultimately came through their proxy. I came to understand that this is more common now than ever. Usually the giveaway is stale data that refuses to be purged, even if you try to delete your temp files, you know, if you kill your caches and cookies, and you reboot, and you do the one-legged hop and retry. I've found at least one other ISP, my current one, appears to be using transparent proxies. Now, normally this would just be an annoyance. But I seem to recall earlier Security Now! episodes in which you mention SSL traffic terminates at a proxy. In last week's episode you mentioned that these invasive ISP tracking solutions can't sniff on SSL traffic. My question is, would this be true even where transparent proxies are in play by that same ISP? I'm still trying to wrap my head around SSL tunnels and have to go back to reviewing older Security Now! topics. But in this world of Trust No One, TNO, I like being extra cautious. By the way, I bought SpinRite, and I think it solved a problem for me. Boot-up issues auto-magically disappeared on my mother-in-law's - he says "mother outlaw's" - PC. So first, what's a "transparent proxy"?

Steve: Okay. This is something that ISPs do in order to minimize their bandwidth usage to their upstream providers, and also theoretically to improve the performance and experience of their own users. The idea is they are - it's called a "transparent proxy" because the users behind it, meaning the ISP's customers, you and I and everybody, for

example, who has a cable modem or in some cases a DSL system, we don't configure to use a proxy. We just use the IP that we're given and believe that we're connecting directly out to remote servers.

It turns out, however, that that's not the case. There is a hidden proxy server which the ISP has interposed in its network for the purpose of caching. So the only reason that an ISP would do this is for caching web content. Again, the idea is that, for example, if you go to CNN.com's home page, well, if I go there I pull the home page. And in the process I use the ISP's bandwidth that it's purchasing from its upstream provider. Remember that ISPs are just Internet users and customers like we are, they're just bigger. So the ISP is purchasing bandwidth, just like we are, except they're bigger. So they're aggregating...

Leo: They buy it wholesale.

Steve: Exactly. However, they still want to minimize their overall bandwidth usage. So the idea is that if I go to CNN.com and pull down CNN's home page, if other ISP customers do the same thing, this transparent caching proxy will notice the URL that is being retrieved and will also look at the so-called "metadata" that came with that page, for example, the expiration time. And if the page which it has cached has not expired, that is, CNN sent it saying, oh, let this page last for an hour, for example, that has the added advantage to CNN of removing the burden from its servers, so it's not having to reserve the same home page over and over and over. It sends out a single copy that has an expiration, for example, an hour in the future. And then the ISP's cache will hold onto it. Then other ISP customers who go to CNN, they get it instantly from essentially what is a local copy of that page in the ISP's cache. Now, that's the good news, when everything works correctly. However, Brian in grumbling about this noticed that sometimes you get stale data that refuses to be purged even if you delete temp files and so forth. And the reason is there's nothing you can do locally to force the remote transparent proxy to update itself. That is, it thinks it knows better. And normally that's the case, that is to say that normally things are going to work well, and servers will be issuing pages that are pre-expired if they never want them to be cached by an intermediate caching transparent proxy.

He also asks about SSL. The good news is that if you use an SSL connection, unless there's been the deliberate installation of a certificate in your browser that we have talked about which is what's necessary in order for an intermediate proxy to be able to intercept your connection, unless that's done you will avoid the ISP's transparent proxy. I had some experience with this years ago when I was first developing ShieldsUP! because my own local cable modem supplier, Cox, they use a transparent proxy. And so when I was connecting to ShieldsUP!, I would be getting the IP of the proxy and be testing that, which of course is not what we want. We want to test the user's actual machine. So that's why ShieldsUP! runs customers, people who come to ShieldsUP!, through a secure connection specifically to bypass ISP transparent caching proxies, which are unable to intercept secure SSL traffic. And they really don't want to. I mean, the notion there is that there's some reason you've established a secure connection, one being that you want absolute privacy and end-to-end security between your browser client and the remote server that you're talking to.

Leo: So he shouldn't worry about it.

Steve: Well, it does mean...

Leo: You have to trust your ISP, I guess.

Steve: Well, and I should say we've got a number of questions that we will be dealing with this week that are offshoots from last week's topic about ISP spying, privacy and betrayal, which caused a great deal of interest among our listeners. So it is the case that given that when you have a nonsecure connection, that is, non-SSL traffic or non-VPN traffic, that everything that you transit through your ISP is available and visible to them.

Leo: That's why we didn't like that Opera Mini browser because that would do the same thing, would proxy your browser. But AOL has done this for years. This was how AOL speeded up browsing. And a lot of ISPs do things like re-encode or recompress graphics and so forth. Lot of times when you get a dial - this is the old days of dialup. But you'd get a dialup provider would say, oh, we're faster, we have turbo speed. And that's all they were doing was proxying, caching, and compressing, recompressing.

Steve: Yes. And you're right, the thing that's different about the Phorm or NebuAd or Adzilla or all those nightmares we first started talking about last week is that in this case, that is, in those cases, ISPs are deliberately sharing this information with a third party. And that's not good.

Leo: Your ISP knows a lot about you no matter what. You really should find one you can trust.

Steve: However, what you would like is that you would like for it to take a court order for them to divulge any information, rather than a commercial opportunity to sell a profile of you to third-party advertisers.

Leo: Right. Tim McCoy in California worries about, quote, "acceptable levels of hard drive failure," as if any level would be acceptable. He says: Steve, I've noticed that some hard drives have close to a million seek failures, or CRC errors, as revealed in the S.M.A.R.T. System Monitor. This noticeably, he says, affects system performance. This does not seem acceptable to me, but how do we convince manufacturers they should exchange drives with such a high rating? Secondly, SpinRite appears not to work with USB keyboards. Is there an update? Let's take the first part of that.

Steve: Yeah. It is unfortunately the case that there has been some cost associated with the insane explosion of hard drive storage capability. And we've talked about this before. These ECC, Error Correction Code, or sometimes known as CRC errors, are occurring at a much higher level, at a much greater rate than they used to because the data is so densely stored now on today's contemporary drives that drives literally depend upon this ECC, the on-the-fly error correction, to correct sectors which are not perfectly readable. It's somewhat troublesome, but it's the way things are.

Leo: You don't have any choice.

Steve: Yeah, there have been other instances where drives are, because of the incredibly high track densities, this is where seek errors are coming from. Drives are having a hard time staying on track, that is, that they have the technology to do what's called "track following," where the head is tweaked on the fly to keep itself over the track. That has to be done because the tracks are so dense that even minute variations in track position cause the head to go off track. It turns out that drives are becoming increasingly sensitive to the vibration of their own chasses that they're mounted in. And I'm seeing now drive manufacturers specifically talking about, like, having extra quality tracking technology in order to help them stay on track. So these are side effects of buying a trillion bytes of data in a small little box.

Oh, and as for SpinRite and USB keyboards, it is the case that SpinRite is still using the BIOS, as we've spoken of, which is universally supported by the older style PS2 keyboards. Most motherboards will have an option, they normally call it "USB Legacy Mode" or something like that, where you're able to - they're able to provide transparent operation of a USB keyboard in the BIOS so that you're still able to use SpinRite with no trouble. But if that's not turned on, you just need to go into the BIOS and set legacy mode for USB support, and then SpinRite can work just fine.

Leo: That's good to know. That's good to know. Jake in Minnesota asks Firefox to forget all about him, forget I was ever here after every use. It's a little setting in Firefox. Steve and Leo, ever since I got Firefox for the first time I've been using it with that Clear Private Data option every time I quit. I've set it to clear everything, including cookies. Is this a secure way to browse, if I don't mind missing the benefits of using cookies, or am I just fooling myself? Thanks for the great show. It's a huge comfort knowing you guys are there making sure we stay informed about security issues.

Steve: Yeah. That is certainly an option for surfing securely. And I know that Firefox does what it says it's going to do, that is, it removes all the sorts of histories of your use which it's otherwise maintaining. And he mentions it also includes cookies. So it does, when you set that, it prevents Firefox from storing that data on the hard drive. It just keeps it in RAM so that when you shut down Firefox, that data is lost. And so it's absolutely a useful and good feature of Firefox.

Leo: Is it a security benefit, though? I mean, is it - I mean, it's a privacy benefit.

Steve: Yes. And I think it's a very good point, and worth drawing that distinction. I think that you could argue that there are ways that security could be compromised when privacy is compromised. But I sort of think of them as separate issues. On the other hand, well, no, I was just going to say, you know, having someone else take a look at URLs that you've visited, you know, how often when you start typing a URL it pops down a list of various things it has in its history that it remembers, you know, locations where you have gone to, in order to help you with sort of autocompletion. So clearly there again is a - you might say that's a security vulnerability that somebody else who had physical access to your computer could see what you've been doing. But it's also certainly a privacy concern.

Leo: Right. Chris W. in Springfield, Virginia has a note about Firefox 3 and cookies: Steve and Leo, I have been a long-time listener, really like the work you do and have been a SpinRite owner since v3, three versions ago, and now have been hoping for a Mac version since I just switched to a Mac (grin). I noticed that Firefox has third-party cookies enabled by default. I was a little disappointed to see that was the case, for the sake of the people who need the most help, the non-techies. Why do you think Mozilla did it this way? Is it a nod to advertisers? Why don't they make third-party cookies off by default? Safari does that on the Mac.

Steve: Yes. And Safari is the only browser, the only popular high-end browser that does have third-party cookies disabled by default. I don't think it's a nod to advertisers at all. I wouldn't believe that the Mozilla folks would be nodding to advertisers. My guess is that if it caused a problem to ever have third-party cookies turned off, then Firefox could be dinged a little bit and believed to be less compatible or to have some incompatibility. It is certainly the case that traditionally, historically, all cookies, first-party and third-party, have been enabled by default. And so I just think it's the Firefox people not wanting to break something.

Leo: I'll give you an example, a really good example, and I was very disheartened by it. There's a Firefox extension called Foxmarks that syncs my bookmarks. It doesn't work if third-party cookies are turned off.

Steve: Yes, and I think we actually have someone mentioning that later in this episode.

Leo: Oh, really, okay. So I think that that is exactly what it does is it breaks stuff that relies on it, stuff you may not, you know, assume relies on it. I mean, and so for that reason they probably default to the - this is always the case. People almost always default, unfortunately, default to the less secure but more convenient choice. They don't want to do support. They don't want the calls.

Don in Burbank loved this week's episode, or actually last week's episode on ISP Betrayal. I love that. Hi, Steve. Excellent show last week. I'm jumping the gun, but what are some simple ways to thwart NebuAd? We're going to be talking about more of that next week; right?

Steve: In detail. We're going to go into the technology of Phorm, which is just a - it's a horror.

Leo: Right. He says: Charter Communications is my ISP. And we talked about that last week, that they are using NebuAd. Using a proxy like Anonymizer or a simple proxy, would that work? Would a VPN like Public VPN? Can I write a program that can pollute the data stream, randomly looking at different web pages? That's interesting. Is there a legal action I can take against Charter? Should I switch my ISP? Is my Yahoo! webmail being spied on? Just a suggestion, could you lay out different levels of thwarting the spying? Level one would be easy, level two a little work, level three requiring good tech knowledge, level the hardest but will stop spying. What do you think?

Steve: Well, okay. First of all, the good news is that any kind of encryption blocks this completely. So it is only the nonencrypted connection...

Leo: Oh, that's interesting.

Steve: Yes. Any kind of encryption. So SSL using HTTPS, if you're able to. When he asks about is his Yahoo! webmail being spied on, if you're able to, as you are with Google and Google Mail, to establish an encrypted connection to Yahoo!'s webmail server, then you are absolutely safe from any of this eavesdropping. Now, they are currently saying that they are only intercepting port 80 traffic. Meaning that, for example, SMTP and POP transmissions, that is, outgoing mail from you to your ISP's web server, I'm sorry, email server on port 25, or incoming email on port 110 or 143 for IMAP, those are, I mean, no, 145 IMAP?

Leo: 143, I think. That's a good question. I think it's 143.

Steve: Anyway. So the idea being that they're saying that they're only looking at port 80 traffic. I'm worried, frankly, about the notion of email being profiled in the same way because think of the wealth of so-called behavioral profiling data that would be available from looking at people's email and doing keyword searches and so forth on that in order to further determine who they are. They can say, oh, no, it's innocuous, you know, all you're doing, all that's happening is you're being categorized into, you know, one of a thousand broad categories of general interest. It's like, yeah, okay, but unfortunately it seems that available information is being taken advantage of wherever it's available. So that gives me a very creepy feeling.

Leo: Yeah. And Google, I mean, look, Google's doing that with your Gmail. There's definitely valuable information in there, they say, in your Gmail account.

Steve: Yes. However, in that case, to address that, for example, Google's doing it with your email in order to show you ads on the Google Gmail pages that are relevant to you. Right?

Leo: Right, right.

Steve: So there's some containment there. You know, the entity that you're transacting with knows about your past usage of email and is saying, look, here's some ads that you may care about. Of course what's different is they're not selling that off to some third party to do with lord only knows what.

Leo: Right, right.

Steve: So the bottom line is any VPN, any SSL connection, anything you do to encrypt your communications is going to completely bypass these guys.

Leo: Yeah, so if you use something like Anonymizer, or if you used something like...

Steve: Or the TOR network.

Leo: TOR, the Boss, these things, the iPhantom technology, all of these are basically encrypted out of - from your browser to their host. Now, of course you have to trust them because they unencrypt it, then pass it along.

Steve: Yeah, there was that wacky little thing, too, called iPig, which had the unfortunate name.

Leo: I don't know what that is.

Steve: It's like it was - we talked about it years ago. Internet something, I mean, it's an acronym [iOpus Private Internet Gateway] that's unfortunate, iPig.

Leo: It is very unfortunate, yeah.

Steve: And it's a little freebie you can download which encrypts your connection to them. I remember vetting the security of it, and it's a nice solution. They're not doing a complete VPN. They're just scrambling the traffic between your machine and their server, whereupon they let it out onto the Internet. But all you really need is you need it just to be encrypted as it passes through your ISP. And once it gets out of your ISP's grip, then it would, for example, go to the iPig servers. And the thing that's nice about it is that it's free. I think there was some bandwidth limitation for how much bandwidth you could move. So you weren't - you didn't want to be doing, you know, big music downloads for that. But for casual web surfing and email, that's another option which might make sense.

Leo: Pretty cool, actually, iPig [snorting]. Oh, listen to me, I'm sorry.

Steve: Thank you for the sound effects, Leo.

Leo: Had a little snort there [clearing throat]. Dan Hunt in Central Queensland, Australia, has been hunting for the PayPal one-time-use credit card. Hi, Steve and Leo. I've been trying to find the PayPal one-time-use credit card for a couple of weeks off and on now. Now matter where I look, I can't find it on my PayPal account. I had the same trouble, I was kind of searching for it, but I found it. He may have other reasons why he can't find it. Earlier this evening I was having another fruitless search when I clicked on the Upgrade My Account link because I thought, what the heck, maybe it's under there. PayPal wanted me to upgrade to a Premier account so I could accept high volumes of payment traffic and all that good stuff.

I was about to navigate away when I had a sudden epiphany. What if, I thought to myself, Steve and Leo have different levels of account than I do? Certainly with you buying cool security gadgets, Steve, with your PayPal account, maybe you've been upgraded to handle the traffic level and probably avoided excess fees. My question is, are either you or Leo on basic PayPal accounts? If not, do you know how we poor, lowly basic accountholders can even use the one-time credit cards? I wouldn't think that PayPal would withhold something so useful from basic accountholders. But I have little luck finding any information about it in the PayPal help sections. Of course it could just be that since I'm from Australia, PayPal may not be sharing the cards over there yet. That's what I thought it was. Is it? What is it?

Steve: Okay. My guess is that's what it is. What I wanted to tell him was that the one definite place to look is see if you can see PayPal Plug-in. That seems to be the most visible, apparent, obvious place to look for this.

Leo: And they're promoting that like crazy, by the way.

Steve: Yes. And, I mean, I just logged into my PayPal account this morning to verify where this was located and how visible it was. And it came up like...

Leo: You can't miss it.

Steve: ...full, huge screen in the front of me. So there was no way to miss that. So I would suggest that Dan take a look for the PayPal Plug-in. And that's where the Secure Card technology is located. Now, I want to take this opportunity to mention a little experience I had since we talked about the PayPal Plug-in and about the Secure Cards. I mentioned during the first time that I discovered it that I enjoyed using a one-time use, or single-use, as PayPal calls it, card on a website where they were sort of like forcing me into a subscription monthly renewal thing that I did not want. but there didn't seem to be any way to opt out of it. So I thought, well, that's good. The bad news is, they recognized, their bot recognized that my expiration date was next month, and they snuck in another charge. Now, I was really annoyed because, first of all, this says "single-use." So I was assuming that the card died after its single use. It turns out it does not. So what I discovered in today's logon...

Leo: Oh, that's interesting. So they could use it within the time period before the expiration.

Steve: Yes.

Leo: Oh, that's not single use to me.

Steve: No, it's not. It's certainly limited use. It's like, you know, this month use. But it's not single use. And what's interesting, then, when I went to the Secure Cards tab under the PayPal Plug-in, it shows you all of your still live cards that you have, then the option

of setting a checkbox to select them and manually close the card. So I wanted to inform our listeners that PayPal's single-use cards are not single use. They stay alive for multiple uses until, presumably, the expiration date is passed. And so it is incumbent upon the user to manually shut down the card when they want it no longer to clear.

Leo: Oh, boy. That's, see, that's not single use.

Steve: No, and it's called "active." You have, like, active cards, and then you manually go there to deactivate the card. So anyway, it bit me. It wasn't a very expensive bite, but it was annoying. And now I know better. So I wanted to pass it on to our listeners.

Leo: And I'm pretty sure we both have Premier accounts. I don't know, is that the one where you have to give them a bank account to make it a Premier account? What exactly...

Steve: No. That's a verified address account. I don't know exactly what number, how they refer to it, what their term is for that. But I may - I'm a verified PayPal user, meaning that I had to give them my bank account information and an address. And so I have a verified shipping address, which some sellers, for example some eBay sellers require you to be PayPal verified or they just won't - they won't sell anything to you.

Leo: Right, yeah, no...

Steve: So I have that. My guess is that it's just an Australia thing.

Leo: I'm looking, too, and I see I'm verified. I'm not Premier. So, yeah, it's an Australia thing. And if you think about it, that makes sense because credit cards are handled differently in every country. They just can't, you know, that makes perfect sense. I understand.

Steve: And you have laws and regulations and all that mumbo jumbo.

Leo: Right, right. Yeah, by the way, verified is probably a good thing. If you're going to do business with anybody on PayPal, make sure they're verified.

Steve: Although the problem is, once you're verified, then you're in that eternal PayPal wants to take money from your checking account mode with no way to override that and have them default to your credit card. So every single time that I do this - oh, and of course the other problem with the single-use credit card is there's no way to redirect that back to your credit card. It insists upon taking from your checking account. So it's probably not even available unless you're a verified user.

Leo: That's interesting. Wow. Yeah, PayPal has some frustrations in it.

Steve: Yeah. Like I said, there's no company more than PayPal that needs good competition to come along.

Leo: Yeah, no kidding.

Steve: And I have to say, though, I really do like Google Checkout. I'm now using - I'm using it more and more because it's a simpler form. It's becoming more widely used. You register yourself in the same way, giving them your own real long-life credit card and your shipping data. But it's a single-click checkout where Google provides not only the - they privatize, keep private from the vendor your account information. They merely do the electronic transfer. But they also provide the shipping address. So it's just, you know, it saves you filling out a form yet again if you're someone who's buying a lot of stuff, physical goods over the Internet.

Leo: eBay has announced that they're going to improve the buyer protection on PayPal. Just right after I got ripped off.

Steve: Whatever happened with that, Leo? I mean, is it still...

Leo: It's still, you know, I escalated it all the way into a dispute, and they're investigating it. But I don't have very high hopes of getting my money back. Because the seller had only insured it - I wish I'd paid a little bit more attention. You know, I knew enough on eBay to look to make sure that he had 100 percent rating and had done a lot of transactions. But there was also a little giveaway which was that he'd only insured the transaction with PayPal for 200 bucks. It's the seller's responsibility to do that. And it was a $2,150 camera by the end of the auction. And I wish he'd insured - well, he's not. He's a crook. He's not going to insure it for anything. I'm surprised he had 200 bucks insurance. He didn't want to spend the extra money on the...

Steve: Now, if that was off of your credit card, are you not able to challenge that charge?

Leo: But it wasn't. It was out of my PayPal account. That's why you want to use a credit card. You're exactly right. Had it been a credit card, I'd have no problem. And it's up to PayPal now to decide whether they want to pay me back or not. And I suspect what I'll get is a check for 100-some bucks minus their fees out of the 200 bucks insurance and that's it. And so they, you know, because - in Australia it's interesting because they're trying to encourage - they want to make it so you can only pay for eBay purchases with PayPal because they own PayPal. And the Australian Consumer Commission turned them down. So I think this is in response to that. They're adding to the protections, they're increasing the amount that PayPal will be liable if you get ripped off, that kind of thing. Too late for me.

Steve: Yeah.

Leo: Matt, his real name is Mariusz, but Matt Cybulski in Newcastle, Ontario, Canada is asking about Hotspot Shield. Hello, Steve and Leo. I just finished listening to SN-149, ISP Privacy. And I've been wondering if there could be a bit of hope left for anonymity online. I've downloaded and installed Hotspot Shield - HotspotShield.com - and ran my computer through ShieldsUP!. Everything except Ping Reply came back as stealth. And even the unique string that identifies my computer came back as "Internet connection has no reverse DNS." Even my IP address changes from one that is issued to me by my ISP. Wow. So does that mean I can't be tracked by my ISP? Of if I can is it then limited somewhat, and what would the limitations be? Also while using Hotspot Shield should I be concerned about the tracking technologies that you mentioned on your last episode, NebuAds and Phorms? Please, if I'm missing something, I'd love to hear about it. There's nothing worse than a false sense of security. I agree. I love your shows, and I occasionally revisit them as this is the one show that makes me put my propeller hat on. In fact, sometimes it gets so geeky I need to hear it more than once. Keep up the great work. That's why we have the transcription, so you can read along.

Steve: I wanted to mention, I wanted to bring this up because Hotspot Shield is a nice-looking solution for exactly this problem. It is free. There is a total bandwidth usage limit. I believe that they run a rolling 30-day window through your usage. And so if during any 30-day period of time you hit a certain bandwidth cap, then they'll say, okay, no more. But you are able to purchase additional bandwidth. So their hook is that, you know, they get you into their service by making it free. You download a little client which you run in your machine, which redirects all of your traffic, encrypted, to them, very much like the other similar HotSpot type of technology we've talked about before. And only if you are a massive bandwidth user do you run across their ceiling. And then if you decide to, you're able to pay in order to get additional bandwidth transit. So HotspotShield.com is a solution which, by encrypting your traffic past your ISP, as it flows past your ISP, prevents you from having to worry about any of this kind of snooping going on.

The problem is, as with any of these sort of third-party solutions where your computer is terminating - and the same is the case, for example, with iPig - is you're going to see some performance hit because depending upon their bandwidth and how busy their servers are, all the traffic is going to them first, then coming to you, as opposed to going directly to you. So it's probably not going to be any faster. It will be somewhat slower. The question is, you know, how much is somewhat.

Leo: By the way, Bull Durham in our chatroom sent me the address for iPig. It stands for iOpus Private Internet Gateway.

Steve: There we go. That's the exact...

Leo: Yeah, it's still around. It's iOpus.com is the company that makes the iPig. Bad name. But as you say, good technology. So this is somewhat similar. I don't understand exactly how Hotspot Shield works. Is it a firewall? Or is it a VPN?

Steve: No, it's just - it's a lightweight VPN solution.

Leo: Okay, okay. And iPig is not, but has some of the same features.

Steve: Well, no, it is also. What I remember from iPig was that the author and I exchanged some dialogue back when I was originally checking it out, and I participated in their online forums because I wanted to understand - it wasn't very well documented, so I wanted to understand what it was that he was doing. There are some instances where NAT-sensitive protocols like FTP would not function. And when I mentioned that to him he said, oh, that's why FTP doesn't work. And I said, uh, yeah. So there are some things that it'll have problems with because it's just intercepting your traffic and sort of moving your traffic over to their server and then emitting it again. And he's just changing the IP on the outside of the packets so that they come back to them. The problem is, so it's not performing a full packet-inspecting NAT operation, which, for example, our NAT routers do. So there are some things that won't work quite right. But things like web serving and email it will have no problem with.

Leo: Okay. That's the frustration about these solutions is if things don't quite work right, it's kind of like, how long are you going to put up with that before you go, I'm turning this off.

Steve: Yeah, exactly.

Leo: Carol - I'm sorry, Chris Noble in Wellington, New Zealand notes that some third-party cookies are needed. Oh, here's the...

Steve: Here is the comment.

Leo: Here's the comment. Hi, Steve. Just listened to your latest episode of Security Now!, heard you mention about third-party cookies in Firefox 3. I, too, am glad I can disable third-party cookies again. You might like to mention to listeners this will break some very useful add-ons, in particular Foxmarks, which Chris and I both use for syncing bookmarks between different Firefox installs, and Google Reader Notifier for alerting you to news items in your subscribed feeds, new news items. Both of these add-ons require cookies to function. And these are treated as third-party cookies by Firefox, presumably as they're set without actually being on the respective websites, which is the exact point of the Google Reader Notifier in particular. The solution is to leave third-party cookies disabled but to add - ah, I'm going to do this right now - Foxmarks.com and Google.com into the exceptions list as allowed cookies, whitelist them on demand. There may well be other add-ons that require cookies in a similar fashion, but these two are probably among the most widely used. Thanks to you and Leo for a fantastic resource in your weekly shows. Please keep up the good work. That, I was going to look for that capability, actually.

Steve: Yes. And so we will be talking here before long about cookies in painful detail, coming up with some strategies for people who want a sort of not-in-your-face, quick solution. And there are people who are willing to do a little more manual cookie management, who really are more concerned about just really not having anyone able to easily track them on the 'Net. And so this is going to work out well because next week

we're going to talk about the Phorm system that has just, I mean, it is cookie overload on steroids, which is what they do to you. We'll explain how that works. And then not long from now I'll finally be able to unveil the work I've been doing on cookie management at GRC. And that'll be the forum for talking about some strategies that people will be able to use in general for managing their browser cookies.

Leo: I'll defer this till then, but I'm really curious as to really how dangerous cookies are. And if they're really, I mean, people really get crazy about cookies and worried about cookies. And I know that third-party cookies are.

Steve: Yeah. And I agree with you, Leo, it's like my feeling is, with very few exceptions like you've just mentioned, for example Foxmarks, you just don't need third-party cookies. And they're so easy to disable. And just doing that, and then whitelisting the very few of them that you might need, solves the problem. And it's just, like, they should be off by default.

Leo: Right. Well, I've just changed my browser, as we were talking, to exclude - to accept third-party cookies from Foxmarks but no one else.

Steve: Cool.

Leo: Joshua Brickner in Loveland, Colorado had some interesting questions about data erasure. He says: Hi, Steve and Leo. My question is regarding recovering erased data on a hard disk drive. I've heard on your show that it's possible for data recovery labs to glean erased data from hard disk drives even after a 35-pass erase, using forensic technology. Did we say that?

Steve: No. So the first thing I want to do is to correct that mistaken impression from Joshua. But go ahead, and I'll do the whole thing at once.

Leo: Okay, we'll do it all at once. Let's say you have two hard drives, we'll call them A and B. Hard drive A had sensitive data on it, but that data was purposely removed using a 35-pass erase. After that...

Steve: And 12 months later...

Leo: No kidding. After that, hard drive A was then repurposed as an everyday, nonsensitive drive. Later on, hard drive A is backed up to hard drive B using Time Machine on OS X or some other backup program. Do the traces of sensitive data left over from before the 35-pass erase that are supposedly there get transferred onto hard drive B during the backup? Or are they unique to hard drive A? Would both hard drive A and B need to be destroyed to be truly secure? Just curious. Love the show. So he's asking, if you backup a drive, and there are forensically detectable traces of previous data on the original, does that get backed up, as well?

Steve: Exactly. That's the question he's asking. Okay, so first of all, relative to data erasure, we absolutely know, and it's been confirmed, that if you simply wipe a drive with zeroes, for example, you just do a low-level format of the drive that just writes zeroes on the sectors, we know that it is possible for that most recent erasure to be penetrated by somebody, a forensic data recovery company that specializes in doing so. However, if you write a couple passes of pseudorandom data, just noise, every time you write, you are suppressing what was there before.

Leo: These are like electrical traces that are left around; right?

Steve: Yes, yes. The idea, it's like imagine an audiotape recording, the old-fashioned reel-to-reel days. If you recorded something on audiotape, and then you recorded silence, you re-recorded over the audiotape, and you just recorded silence, it was possible for technicians to pull the previous analog recording out of the background noise.

Leo: Right, right.

Steve: Sort of like a really, really faint whisper so that - because it was analog data that was written over previous analog data. Well, even though hard drives are digital technology, the actual waveforms that are being written are so tightly packed together that the square waves meet each other, and you're actually recording something that is more analog-like than it is digital.

Leo: Oh, interesting.

Steve: So there's a whisper of the previous data from before, just faintly in the background. And if you know what the foreground is, and you subtract that from what you are receiving or reading back, you can - that whisper is still there, very, very faint. And if you then amplify that, you can recover from one, certainly from one prior erasure. It is not the case, however, that you can do that after you have written random noise a couple times.

Leo: A couple of times. Not even 35. Just two or three times.

Steve: I really - yes, two or three. And so the whisper that you would recover would be the previous noise. And then if you tried to remove that, I mean, at that point it just, I mean, two passes is almost certainly enough. Okay. Then his second question is, if you were to read the data from drive A and copy to drive B, is any of that whisper going to be copied across? And there the answer is an absolute, definitive no. Because the whole point of a drive is to only return the most recently written data. And it's all digital. So that all of that little whispering I'm talking about, that exists only inside the drive. And always what the drive is going to return is nice, clean, digitized results, which is the actual digital data that goes across the cable to the motherboard. So when all of this forensic magic is being done, they're not doing it at the regular connector that we connect to when we interconnect our motherboards to drives. They're in there reading analog data off the heads before the drive has a chance to digitize it back into ones and

zeroes in order to have a chance to pick up this whispering data which the drive immediately clobbers and only returns to you what was most recently written on the sector. So there's no way for those whispers to get across to another drive.

Leo: Just not going to happen. Don't worry about it. Rob in Southern Illinois is not happy about next-generation behavioral tracking and profiling systems. He says...

Steve: And nobody is, by the way.

Leo: Yeah. I'm happy, well, the people who make them are happy about them.

Steve: I don't think even they're that happy at the moment because this has really caused a big storm.

Leo: If they're happy, they should stop being happy right now. He says: Hi, Steve and Leo. Regarding your podcast about ISP Betrayal, I'm very disturbed by this technology. If access is given to all traffic, email is an example where a lot of data can be gathered and used for who knows what. The majority of PC users do not understand email is plaintext in most cases. This technology would give access to all kinds of information in emails, including usernames, passwords, personal information, confidential information, et cetera. This is plumb scary to me, both personally and professionally. This technology should be stopped, in my opinion. Thanks for the awesome podcast. P.S.: Steve, SpinRite's saved the day many times since I purchased the software. Keep up the great work. Hey, can I just say one thing? If you're sending email and not thinking of it as just like sending a postcard, you've got the wrong idea anyway. You're assuming your email's secure, come on. Right?

Steve: Yeah. Although I think the point that Rob is making, and this is I think what really put a chill in people, is that when an ISP begins this kind of profiling, they're really on a slippery slope. I mean, they're trying to say we're just a bandwidth provider. We're not going to prevent porn or spam or hacking or any kind of obnoxious behavior. We're just a common carrier. And there's a formal definition for what a common carrier is. And part of what - essentially they're saying we're taking no responsibility whatsoever for the content. We're just providing you the bandwidth. Well, suddenly now they're saying, ah, but we're going to make some money by selling profiles of you to a third party. Well, that really does change the nature of their relationship with their customers.

Leo: Well, I agree with you 100 percent. But even if none of this were happening, I mean, anybody who sends data through email is asking for trouble because it's not just your ISP. It goes through a bunch of servers. And it's unencrypted. It's in the clear.

Steve: Yes. And you might also note that even if you had a secure connection to your ISP or to even a third-party email server, well, when it's collected by the other end it's going to be in the clear. So...

Leo: That's why, you know, if you're not encrypting your email, you must consider it publicly visible. It's like sending a postcard.

Steve: Yes. If you are not doing end-to-end encryption, where you encrypt it before it leaves your machine, it's a pseudorandom blob of noise during its entire transit between multiple email servers. And then your recipient receives it as a blob of pseudorandom noise, which they then decrypt at their machine back into plaintext. That's the only way for email to be safe.

Leo: PGP or the like.

Steve: End to end, yes.

Leo: I use a Gnu - it's called Gnu Privacy Guard, GPG. It's free, it's open source. And for instance, the guy who does our TWiT site, Gordon Heydon, he's a great programmer, he's in Australia, Drupal expert. He said, can you send me the root password for the server because I'd like to upgrade PHP. Well, you'd better believe I encrypted that email to him. You just, I mean, email is not secure. So let's not assume it is secure or it's suddenly become insecure because of your ISP. It never has been.

Question 12, Mark De Nardo, Bethlehem, Pennsylvania wonders about possible new trackers in email: Steve, in getting copies of email to my Blackberry, the Blackberry doesn't offer HTML viewing of email. By the way, enterprise device, that's why. Good thing. So I can see the email source. I've noticed a company called MX Logic - this is the company that we subcontract our corporate email spam scanning to - is supplying graphics on several emails, but the name of the graphic is blah blah blah images slash transparent.gif.

Steve: Yeah, but notice it's portal.mxlogic.com.

Leo: Okay. So the graphic is coming from their site.

Steve: Yes.

Leo: Why would an email have a transparent graphic? Is this another counter/tracker scheme? I'm also a bit disturbed the Outlook, Outlook Express and Windows Live Mail won't let me read my mail as text-only so I can see these types of hidden graphics. And finally, if I may, I'd just like to say I drive an hour each way to work daily and listen to Security Now! and several other netcasts provided by Leo and TWiT.tv. I enjoy the way you and Leo share your knowledge. I'm a 50-plus-year-old geek who's been able to take his hobby with computers and make a career of it in the corporate world. Yay, Mark. Also a proud owner of SpinRite and have found it very useful over the years. So, yes, this transparent GIF, you see them a lot now.

Steve: Well, yes. And this is absolutely tracking. And this is why I'm so down on third-party cookies. This is, I mean, this is what third-party cookies allow is that when your browser opens this image, it's going to pull this, and this MXLogic.com is going to know that you viewed the file. Now, we have to presume that - he said that this MX Logic is the people that this company, his corporation, is having do their spam scanning. So what's a little disturbing is in the process of scanning the spam they are...

[Talking simultaneously]

Steve: Yes, they're modifying the contents of the email which is passing through their spam scanner. And we don't know why. Now, maybe this is part of their feedback. Essentially he said that it's called transparent.gif. We have to assume that there's no visual content there, in fact it's deliberately transparent so that it doesn't show up in a normal HTML viewer. But what that means is that when the email is viewed, their server will receive a little ping. Now, there's no other information in the URL. So it's not clear what information they're going to get except they're going to get the IP of the reader of the email at the time that that email is opened and read. So it's hard to know why they're doing this. But it is a little annoying that they're modifying the email which they are scanning. That's, you know, I'm sure it's in the fine print of their agreement somewhere. But it certainly is the case, I mean, these were called "web beacons" when they first appeared. And apparently this is still going on. There are websites that put these, either one-by-one pixel so that they're not very visible, or they're transparent, and they're used specifically for third-party servers to transact third-party cookies for the purpose of tracking.

Leo: Yeah, I mean, and spammers do this, too. So, and there are...

Steve: So they know if you're...

[Talking simultaneously]

Steve: ...if you're somebody, yes, exactly.

Leo: And it doesn't have to be by your browser because most - and unfortunately most email programs will render an HTML email. They use your browser's engine. In the case of Windows they use Internet Explorer; in the case of the Mac they use the WebKit. They render it using the browser engine. And at that point they pull that graphic down. They ping the server and say, yeah, he's reading it. Got it right now. He's opening it up right now. Of course...

Steve: And they know that then it's a real person that they've got, and not just some random, made-up email address. You just verified that you exist.

Leo: That's the chief value to a spammer, of course. And that's why I know you recommend this, I certainly do it, is turn off HTML preview in your email program. In fact, I really - it's hard to get people to get this, that HTML is a bad thing for email. For so many reasons. For security, for privacy. You know, you can hide where the link comes from, that's how phishing works because the link isn't apparent. You can't see what the link is, it just looks like a good link. It's fat. It makes email messages

much, much bigger. There's just - there's no reason for HTML email to exist. And yet we're moving inexorably in that direction, and all email's going to be HTML now. It's too bad.

Steve: Yes, it is. And of course it can also carry scripts. And the last thing you want is your email to be executed.

Leo: Gee. I mean, who thought that was a good idea?

Steve: Uh, let's see. They wouldn't be up in Redmond, would they?

Leo: Well, to their credit they have, over time, they've disabled this, more and more features of email. And what they've done lately in Outlook and Outlook Express and Windows Live Mail is it will not display a graphic automatically. Right?

Steve: Yeah, and that only took, what, ten years? About a decade.

Leo: But I think they, you know - now, of course, I get a lot of calls to my radio show saying why won't my graphics display? I don't understand it. They should display. No, I think there's a setting in Apple Mail because my Apple Mail does not display graphics. I don't know if it's default or not, but my Apple Mail does not display graphics by default. You have to push a button that says Load Images. So in those cases, if there's a transparent graphic or a one-by-one GIF there, that's protecting you; right? They won't show up.

Steve: Yes, yes, correct.

Leo: I just wanted to make sure that was the case.

Steve: Yeah. They won't show up, they won't be rendered, and they will not make a query out to some other random server saying "ping."

Leo: Hello. I'm here. Honey, I'm home. All right, Steve. We've gone through 12 great questions. We thank everybody for sending those questions. It's really nice to have them. If you want to ask questions for - we don't do it every episode, every other episode. They can go to GRC.com/securitynow and ask them there; right?

Steve: It's actually GRC.com/feedback.

Leo: Feedback, okay. Now, if you go to GRC.com/securitynow, that's where you'll find all of the Security Now! episodes, 150 strong. There are 16KB versions for

people who have bandwidth issues. There are transcripts, text transcripts. I think that's a great way to read along while Steve talks, to understand it better. Many people like to have that visual input along with the auditory input. And don't forget, GRC.com's the same place you go to find SpinRite, Steve's incredible hard drive maintenance utility, must have, and all of his great freebies including ShieldsUP!, Wizmo, Don't Shoot The Messenger - or Shoot The Messenger, actually - Unplug n' Pray - you do want to Shoot The Messenger - and many other great programs. A lot of them, though, the good news is, and I'm sure you're happy about this, no longer necessary because of changes Microsoft has made to Windows, perhaps to some degree in response to your criticisms.

Steve: I don't think that they're responding to me at all. I just think they're moving forward. But for what it's worth, people who are able to use all the freeware that I've written had the benefit of these improvements years before Microsoft got around to it.

Leo: Right, exactly.

Steve: So that's certainly been good. And...

Leo: And there's still places where you want it, like turning off Universal Plug and Play and stuff like that. Still very valuable. You'll find it all there, GRC.com.

Steve: Next week we're going to - I warn people now. Have your propeller beanie hats handy. It's going to be a very deep technical, but really interesting, episode. We're going to go into the Phorm system, which is arguably the most horrific of the systems I've looked at closely that supports ISP betrayal of their customers, and see exactly what it takes to track somebody who doesn't want to be tracked. It turns out what they do is just amazing. And it bypasses third-party cookie protections.

Leo: Wow. This is good stuff. And I love it when we get geeky. So get ready, get your propeller hats on, kids, for next week.

Steve: Gonna have a full geek episode next week.

Leo: All right, great. Steve, thank you for being here. We really appreciate all your help and the great show you do. And we'll see you next Thursday on Security Now!.