SECURITY NOW!

Transcript of Episode #229

The Rational Rejection of Security Advice

Description: Steve and Leo turn everything around this week to question the true economic value of security advice. They consider the various non-zero costs to the average, non-Security Now! listener. They compared those real costs with the somewhat unclear and uncertain benefits of going to all the trouble of following sometimes painful advice.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-229.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-229-lq.mp3

Leo Laporte: This is Security Now! with Steve Gibson, Episode 229 for December 31, 2009: The Rational Rejection of Security Advice.

It's time for Security Now!. This is the show where you will be protected. You will arm yourself against a sea of troubles and, by learning about security, perhaps end them. Or at least prevent them.

Steve Gibson: It will protect you whether you like it or not.

Leo: Our security guru. Actually the topic of the show today is maybe whether you - maybe not.

Steve: True. We have the title of today's show, "The Rational Rejection of Security Advice," why it is not necessarily, that is, in fact, the argument has been recently made that in terms of the actual economics of the cost of following advice versus the cost of not following advice, that it is cheaper just to ignore us and disconnect your iPod.

Leo: We shall find out. I should say our security guru Steve Gibson is here from GRC.com, as always, host of 229 episodes now of Security Now!, entering soon our new decade.

Steve: Yes, this is our New Year's Eve episode, December 31st.

Leo: Last presentation of 2009. Well, this is going to be interesting. I think I'm the poster child for the rational rejection of security advice.

Steve: Yes, we'll have lots of examples actually of, through the last four and a half years, of you saying, well, how big a problem is that really?

Leo: I don't want to do that. I don't want to do that.

Steve: I really don't - I like scripting. I need my scripting.

Leo: Ooh, boy. All right. Well, we'll see.

Steve: So it has been a quiet week since we last checked in with our listeners. Only two little bits of news. There's a new zero-day flaw that has - a zero-day vulnerability has turned up in Microsoft's web server, IIS. And the security community is sort of at odds with itself about whether this is going to be a big deal or not.

The problem, it turns out, is that if the web server is configured to allow uploads of things like images, like JPEGs, to an upload directory - and, for example, you would do that if you had a Web 2.0 site where you were allowing people to, like, upload their photos or their thumbnails or whatever, like to forums or to photo posting sites and so forth. The problem is that there is some technology that protects executability by file extension. So, for example, you wouldn't want .asp, which is Microsoft's active server page technology, to be live in an upload directory because a user could upload code, essentially, active server page code, and it could be run.

Well, it turns out that there's a little bit of a parsing, a filename parsing flaw. If you were to upload malicious.asp semicolon .jpg, that is, essentially you'd have the actual filename would end with JPG, then it would get through the filters. And the way, unfortunately, the way Microsoft's IIS current server currently parses, the semicolon would stop the filename parsing, so the server would see malicious.asp after it slipped under its defenses and execute the code.

Leo: Now, Microsoft says this is only if you're poorly configured.

Steve: Well, yes.

Leo: Like you have to do a stupid job of configuring IIS.

Steve: And thus the argument within the security community. Microsoft is saying not a big deal. There are people who have said, oh, just wait. I mean, there's enough IIS out there, you know, there's enough targets, it's a target-rich environment, that it only takes a few. And if exploitable, then this is really bad. So, and it also takes having an executable upload directory, which is really crazy. I mean, no...

Leo: Yeah, you shouldn't have that.

Steve: No sane webmaster would configure a server so that uploads of images and things that are supposed to not be executable would have execution rights.

Leo: That's how my server got hacked, by the way, a couple years ago. I had an open directory that you could upload to. And the problem with PHP is it's executable. So all somebody had to do was upload a malicious PHP script, and then he could run it. And he found the open directory. And so that was my fault. Badly configured. I don't have those anymore.

Steve: And the point is that it's easy to do.

Leo: Yeah.

Steve: With all of the servers out there, all of the - one of the things that often happens is that a webmaster, in trying to get stuff to work, like if something's not working, his scripts aren't working, they'll quickly or temporarily make everything executable or writable, just to sort of see if that's the problem, intending later to go in and re-restrict the rights. And, oops, what if they forget? It's like they're so excited that they got it working, they then go off and, like, make sure it's working and do other things and forget that the way they got it working was to overly permit rights. I mean, it happens so easily.

So anyway, it's expected that maybe a week or two from now - Microsoft's next Patch Tuesday will be January 12th. So there's some window of opportunity. If they patch this that quickly. They haven't had a lot of notice of this. So anyway, I just wanted to sort of put that on the radar. It may end up getting patched, but nothing will happen. Or two weeks from now when we are again recording - because we're doing a double recording today, recording our second episode for next week, which will be Episode 230. We're recording that also since you're going to be off reporting on activities at CES.

Leo: Yes, yes.

Steve: And my only other little tidbit was, I saw this, and I said, yeah, well, we knew this was going to happen. Kindle's DRM has been cracked.

Leo: Oh, thank goodness. I'm glad about that. I don't like DRM in any situation.

Steve: You know, I support Amazon. I support the Kindle. I carry it with me. I love it. I recently rediscovered the Financial Times, which is something I enjoy because it's got a nice out-of-the-U.S. perspective, and it's well written, and good reporting. It turns out that when Amazon released a PC client, Kindle for PC, that was sort of the Achilles heel because now if this thing, this Amazon client is running on a PC, then all the very mature hacking tools come to bear. We've got disassemblers, we've got decompilers, we've got debuggers, we could single-step, we can catch things mid-load, I mean, there's just a huge mature set of tools which, you know, don't exist for some random little piece of hardware with a funky eInk screen. But boy, you bring the client into a PC environment and, suddenly, good luck keeping it protected.

And, you know, we've talked often about the fundamental impossibility of what Amazon wants to do. You want to give people something which they in the privacy of their own homes can decrypt and read. So the device has to decrypt it to display it, just like DVDs, just like Blu-ray and HD DVDs. I mean, doesn't matter how much huffing and puffing you do, it's going to get cracked because the device in the user's control has to be able to decrypt it. End of game.

Leo: Yeah. The key is built in. You can't hide it.

Steve: Yes, has to be.

Leo: Has to be.

Steve: Yes. So again, what Amazon's trying to do, just like the DVD guys, just like Blu-ray and HD and everything else that will quickly be cracked, is fundamentally impossible. So again, I - and as you said, you don't like DRM. We would argue that, you know, I don't want to steal anything. But it would be nice not in any way to be inconvenienced by DRM. So that, if a book that I buy, I want to read on a PC, what if I want to read it on two PCs, or three PCs? And they're all mine, and I'm the only one going to read it. Well, the DRM starts to get in your way. So anyway, there are two different people who are now claiming that they've cracked it in different ways.

Leo: Is it a practical thing, though? I mean, can you now, you know, share your books?

Steve: Not quite. But it'll, you know, wait three days.

Leo: Right.

Steve: I mean, this is - it's over.

Leo: It doesn't take long. In fact, I'm surprised it took a year.

Steve: There was - actually, apparently it didn't. There were some obscure scripts around that now we're seeing reference to. One user who was posting to the blog of one of these crackers, he wrote, "I've been aching for someone to un-DRM Kindle for PC," this story goes. He says, "A few of my textbooks for this semester and next are only available on Kindle and dead tree." Whatever dead tree is.

Leo: Dead tree is paper.

Steve: Okay. Oh, got it.

Leo: That's what we call - that's what we nouvelle digerati call...

Steve: That's the jargon for...

Leo: ...things printed on paper.

Steve: Got it.

Leo: Dead tree.

Steve: He says, "I have an eInk reader already, not a Kindle. And so I don't want to be forced to buy a Kindle. But the $10 Kindle book is so much better than a $30 paper book. Not to mention it's reflowable, and I can more easily make it fit my eSlick's screen." So he has an eSlick reader, which is a cute little thing from the Foxit people, who of course are a well-known alternative PDF group. And so he'd like to be able to, you know, he's got content that is currently Kindle-only, and he'd like to be able to read it on his non-Kindle reader. Of course that's not what Amazon wants him to be able to do. So this is - he's excited that this is on its way. And you can imagine people being excited for different reasons. So, anyway, I wanted to put that on our listeners' radar.

And finally, what I thought was initially the brilliant tip of the year, but I'm a little less sure of that now. This is sort of in our errata category. I ran across this when I was pulling together the Q&A questions for next week's Q&A episode, which we'll be shortly recording. Levi Stoll in Denver, Colorado offers this cool sounding suggestion for cleaning keyboards. He wrote, "I've been catching up on Security Now! podcasts after a busy year. And I heard Leo talking about washing his keyboards in the dishwasher."

Leo: That was a while ago, yeah.

Steve: "I used to do this regularly, but there's a better way. Key caps, it turns out, are not built to withstand the high heat of a dishwasher..."

Leo: Well, you don't have to use high heat, obviously.

Steve: Good point, "...and frequently warp as a result. I now fill a container with four to six denture cleaning tablets."

Leo: Oh.

Steve: "And use just warm water. Add the key caps, and a few minutes later they come out all sparkly clean and disinfected. Thanks for the excellent podcast. I look forward to Security Now! each and every week, even when I don't have time to keep up." So I thought that was interesting. Now, I did a little poking around, thinking, okay, what are denture cleaning tablets?

Leo: Yeah, what are they? They're fizzies.

Steve: Turns out they're very aggressive. And you might put your keycaps in, and they'd come out all without any writing on top of them. So I'm a little less sanguine about suggesting that to people. Apparently retainer cleaning tablets are much gentler. For example, I ran across some dialogues with people saying, hey, you know, I've been using denture cleaning tablets to clean my jewelry, and boy did they come out all sparkly. And apparently it's, yes, but it's also attacks gold and silver and weakens it and does bad things. So it sounds like maybe those are on the extreme end of the cleaning strength. But it's been recommended that retainer cleaning tablets are more mild and gentle. So, anyway, I just thought was sort of an interesting little...

Leo: Yeah, I mean, we used to - it's funny because in the early days of TechTV for some reason the producers just loved the mouse and keyboard cleaning segments. We did a dozen of them. And, I mean, it's like, they're $5 to buy a new mouse, $10 for a new keyboard. Just buy a new one, for crying out loud. And you pry all the key caps off, you have to take a picture first so you can put them back in the same place.

Steve: Yeah, otherwise you're in trouble.

Leo: Yeah, believe me. It's easy. You think you know exactly where everything goes. But some of those keys are kind of obscure. And it's a pain to pry them off, pain to put them back on. I put them in the dishwasher because it's quick and easy. If it doesn't work, big deal. I buy a new keyboard.

Steve: Yeah.

Leo: But I've washed this keyboard. The trick, as long as we're talking about it, is you've got to let them dry. Don't be impatient to get it back in service. Give it a week, on the edge, dripping.

Steve: Ah, yes.

Leo: Because if it's not dry, you're never - it's never going to work again. So I'm not recommending people do this, please. Don't write me a letter saying, "You broke my keyboard."

Steve: Yeah, I mean, I'm looking at mine, and it just, you know...

Leo: They're grungy.

Steve: It is. It is. I don't even want to...

Leo: You want to dishwash it because just cleaning the key caps - it's not just the keycaps.

Steve: Yeah, I was going to say what's really bad is what slips down in between them and collects over time. It's like, what? It's like alien who knows what.

Leo: Oh, yeah, it's microbial.

Steve: Hairs and skin and, yeah.

Leo: It is, yeah. And so you can just imagine what's growing in there. And the truth is, in an environment like this, where we share this keyboard, you know, I have - there's other people, you know, use this studio. Used to be my desk. Now it's the studio.

Steve: If the keyboard starts walking off by itself, you know that it's time to...

Leo: So this is the Apple Aluminum. It washes very nicely. I've done it twice. It'll probably corrode. But, yeah, don't do it in the hot cycle.

Steve: I'm going to have to - actually a project of mine coming up is to take the guts out of one of my keyboards because they draw so much power. They, like, the house lights dim when I plug this thing in. And because it's old school, it's more than 20 years old. I love it. It's clanky and wonderful. But it's a PS/2 interface. And what I want is not only to have it, give it a USB interface, but also somehow much less power consumption. And so I'm going to end up just taking all the guts out and do my own little keyboard scanner so that I can plug it into a laptop when I'm not tied and tethered to AC power, and still have useful battery life. So I'll spin off sideways and get that done here one of these days. But I'm looking at this keyboard, it's like, oh, just it really does need - it needs some attention. So I'll get around to that. In the meantime, I got an interesting piece of mail with a strange title that caught my eye: "SpinRite Cooks My Bacon."

Leo: I certainly hope that's not a new use of SpinRite.

Steve: From Phillip Nordwall in Bellingham, Washington. He says, "I just wanted to say thanks for your great program, SpinRite, as well as Security Now!. I'm a systems manager for a computer science department, and we have been using SpinRite since the middle of 2008. We have used it a couple of times for data recovery on laptops issued to students. But more notably, we PXE boot 108 machines every quarter for a SpinRite preventative maintenance run. We have cameras in the labs. If you're interested in seeing 108 machines concurrently running SpinRite, just send me an email. Hearing all the testimonials for SpinRite saving people's bacon, I've decided that, when I retire one of my home hard drives, I'm going to attempt to use SpinRite to cook my bacon via a heated drive. I thought you might get a kick out of SpinRite cooking bacon instead of saving it. Thanks for all your work. Phillip Nordwall."

Leo: That's very funny. PXE is the Preboot eXecution Environment.

Steve: Yes. Which essentially allows...

Leo: A lot of machines have now...

Steve: Yes, and probably all new BIOSes do, a way, basically, of booting over the 'Net. And they've got it set up so that they've put together a bootable image of SpinRite which allows them then to boot SpinRite over the LAN. And so, you know, not have to go running around individually booting. I think it's very clever. And they run it quarterly just as preventative maintenance, so that none of those machines in the labs have trouble. And course every so often a student laptop does. He did also in his note - I removed it - he gave me the licensing number and name because they have a site license. So that they're all up and up.

Leo: That's a very affordable and effective way to use SpinRite, actually. That's clever.

Steve: Yeah.

Leo: My laptop has PXE, and it uses it for the preboot authentication with the fingerprint scan.

Steve: Right.

Leo: So it PXEs, and then it runs this, you know, kind of primitive scanner program before I can even access it.

Steve: Your new Dell laptop.

Leo: Yeah, yeah. And that keeps the hard drive locked. Everything's locked unless you - I wonder, though, how, I mean, come on. How effective is that fingerprint scanner really? Can't you spoof it?

Steve: You know, it's funny. I've been wondering, and so I have some of my fingerprints not registered. It never gets fooled by them. And I've had two experiences of, in both cases women, I don't know if it's a sexist fingerprint reader or not, but women who cannot, just cannot register on the thing. I don't know if it's that their ruffles don't have ridges or what is happening. But a gal that I have helped with security and set up - I chose a little Dell laptop for her and was getting her all tuned up and set up, a friend from Starbucks, just she'll - she's got kind of honkin' fingernails, which may be part of the problem. And she's about as computer illiterate as anyone could be. But she really cares about security. So it's very important to her that no one be able to access her computer. And the problem with her fingerprint reader is she can't ever make it happy. And, I mean, I've had her, like, do it on the palm of my hand so I can see how hard she's pushing, and I've watched her do it. And what's so strange is like when she's trying to train it. She'll just stroke it, and it'll say, eh, no. She'll do it again, eh, no. I'll do it once, and it says, oh, good swipe.

Leo: Dr. Mom has a theory.

Steve: Okay.

Leo: Hand lotion. Tell your friend to stop using hand lotion. It fills in the ridges.

Steve: Okay.

Leo: I bet you you don't use hand lotion, Steve. I'm just guessing.

Steve: No, you're right about that.

Leo: I don't see you putting on the hand lotion. But women, all the time; right? And Dr. Mom says what happens - I imagine what these things are doing is they see the bumps and ridges; right? They're bouncing a light off of it. It's almost like a CD reader.

Steve: I think that's actually ridges, but in a different technology. I believe they're capacitive. And so once again...

Leo: But there's a rhythm to the whorls, how many ridges and how close together and so forth. But if your fingers were swole up with emollients, maybe that would affect it. I don't know.

Steve: Well, anyway. So my experience has been, if anything, these things are too finicky and not permissive enough.

Leo: Now, "MythBusters," now, "MythBusters" is not a scientific show. A lot of people bring up stuff like this. They bring up, oh, "MythBusters" proved - and it's a TV show, folks. You know, it's entertainment. It's not science. However, they were able to spoof these fingerprint readers, they claim. Now, the problem is that the technology's changed a lot. The early fingerprint readers, you could spoof them with Play-Doh.

Steve: I was just going to say there's a difference in reader technology. So what I remember from the "MythBusters" spoofing was that it was not the little strip reader like you and I have on our laptops. I've got them on all my ThinkPads and use them and like them. But rather those were the full, press your thumb on this plate kind of reader. And, yes, those are easily spoofed.

Leo: Yeah. Well, I use it. I don't - it's one of those things where, you know, I still have a password, too.

Steve: It's a good thing.

Leo: It's a good thing. Why not. All right. Tell me I'm not crazy. Frequently I listen to you, Steve - and I have to say, you know, I've been here for every show, except for the scariest one which Alex Lindsay did. The next week he said, "I'm never doing that show again. I'm scared." But I guess I'm used to it because I know how scary and dangerous it is out there. But I choose, I think with intelligent forethought, I choose what security measures to take and what not to take. Am I crazy?

Steve: I don't think you are.

Leo: Whew. Thank you.

Steve: What happened was, the thing that sort of put this on my radar is there's an annual, very small workshop which is invitation-only, very small and sort of intimate, called the New Security Paradigms Workshop. The site is, not surprisingly, NSPW.org, New Security Paradigms Workshop dot org. The most recent one was held September 8-11 of this year, 2009, at the Queen's College at the University of Oxford in the U.K. And a paper was delivered by a Microsoft Research researcher, Cormac Herley, titled "So Long, and No Thanks for the Externalities: The Rational Rejection of Security Advice by Users."

Now, to set this up a little bit, I'm going to - I want to read from the introduction page of the site because it gives you a sense for where the conference is oriented. Their introduction says, "NSPW's focus is on work that challenges the dominant approaches and perspectives in computer security. In the past, such challenges have taken the form of critiques of existing practice, as well as novel, sometimes controversial, and often immature approaches to defending computer systems. By providing a forum for important security research that isn't suitable for mainstream security venues, NSPW aims to foster paradigm shifts in information security. "In order to preserve the small focused nature of the workshop, participation is limited to authors of accepted papers and conference organizers.

"As a computer security venue, NSPW is unique in format and highly interactive in nature. Each paper is typically the focus of 45 to 60 minutes of presentation and discussion. Authors are encouraged to present ideas that might be considered risky in some other forum, and all participants are charged with providing feedback in a constructive manner." So, you know, don't laugh at the guy when he's putting something out there that may be contrary to what you're used to hearing.

"The resulting intensive brainstorming has proven to be an excellent medium for furthering the development of these ideas. The final proceedings are published after the workshop, giving authors an opportunity to incorporate feedback from the workshop. The proceedings of NSPW are published by the ACM, a very well-known Association of Computing Machinery. In 2009 we had papers on usable authentication, malware detection, file system access control, and secure routing. We had papers that challenged the foundations of security practice by questioning how we analyze and evaluate security problems." And here's the kicker. "We even had a paper that argued that users were potentially right to ignore standard security advice. The full proceedings for 2009 and past years are available here. Enjoy."

And so any listeners who are curious about other aspects of this, NSPW.org has everything there. Click on proceedings. There's a list of all prior years, 2009. There's a list of the papers from this year. And specifically, this one by Cormac Herley, which when I learned of it a couple months ago, it's sort of just been in the back of my mind, thinking okay, the guy brings up some very good points that we have to discuss because they're issues which have always sort of been in the margins of our discussion. And Leo, as you said, you're often sort of taking a bit of a contrarian position, saying wait a minute, you know, how big a problem is this really?

So Cormac takes a look at - from the whole spectrum of advice sort of stuff. And these are, not coincidentally, here we are four and a half years into the podcast. We've already covered everything pretty much that there is to cover. But he looks at passwords, threats from phishing, and certificate errors, SSL warnings that users get. And when we talk about sort of the economics of following advice, well, obviously we're not talking necessarily in dollars and cents, although in his paper he does go into quantifying the cost in terms of, like, twice the minimum income of a random person and over the course of a year how much time would be spent in doing something versus what the cost would be to not doing something.

So the idea is, in terms of economics, we mean like sort of academic economics, where there is arguably a non-zero cost for following advice. And of course a few weeks ago I talked about the conversation I overheard at Starbucks where there was this executive with his coworkers explaining to them the lengths he goes through to avoid the IT department's password policy. Passwords expire at his company after not apparently very long, and he finds it very annoying that he's being asked to change his password constantly. So he's so determined that he knows better than the IT department about the safety or lack of this policy that he'll go through five other passwords in a row in order to get back to a sixth one because the system remembers the last five and won't let him use any that he's used recently. So they've got a password policy which they're attempting to enforce, but in this case this guy believes he knows better. That is, the hassle that he's being put through, the cost from an economic standpoint, the cost to him of being forced to really change his password is far higher than he believes the expense would be of...

Leo: Getting hacked.

Steve: Getting hacked because he's managed to fight to hold onto the same password forever, essentially.

Leo: Well, that makes sense if it's, you know, your access to your New York Times page. Maybe not if it is to your bank. So different sites have different values.

Steve: Well, yes. And in fact one of the things that I've noticed is I've seen websites where five years ago - Amazon is a perfect example. I've been an Amazon member from, like, day two when I heard about it. It's like, oh, this sounds wonderful.

Leo: Me, too, yup.

Steve: And I confess my first password was weaker than weak. But back then

Leo: It didn't matter.

Steve: ...at the dawn of the 'Net, it was like, eh, who, you know, there's you and I and four other people were on the Internet, Leo.

Leo: Exactly.

Steve: And I trust you. So, and besides, if you want to buy a book, that's fine with me. So when, oh, I know when it was, it was when I was signing up for S3 stuff.

Leo: Yeah.

Steve: I wanted to mess with Jungle Disk and S3. And so I needed to sort of, like, refresh my account. And I tried to just log on as me because Amazon already knew me, and it said, oh, you've got to be kidding. That's your password?

Leo: Well, that's good, that's good.

Steve: And so what happened was over time their policies changed. Now, what probably - if you peel back the covers you can imagine that there were probably people getting hacked because there were people who had, I mean, my password wasn't really bad compared to what it could have been. And in fact, if I think about the absolute lack of enforcement then, people probably had a password of, like, "X," literally.

Leo: Well, you saw - I don't know if you saw, but Twitter just recently banned 300 passwords. They said you cannot create a Twitter account if you use "sex," "12345," "ASDFG," all of the obvious passwords. In fact, it's worth looking at that list of passwords just so you understand what a crappy password is.

Steve: And we also know that that was a consequence of Twitter being hacked.

Leo: Many times. And in fact its own people being hacked.

Steve: And so my point, and you just made my point for me, is that what must have happened is that Amazon was having problems with the fact that they weren't enforcing stronger passwords. And so they didn't retroactively suddenly surprise me one day and say you can't use this anymore. Maybe they would have if more time had gone by. But instead, when I attempted to do anything that gave them sort of an in, they said, you know, we're not good with that anymore.

So in terms of policy, and we've talked about all this before, we know that longer is better because it makes them less susceptible to brute force. We know that varied composition is better - upper and lower case, numbers and letters. We know that things that are not in the dictionary, like the list that you were just running through, not simple words. But then there's other policy advice, like don't write it down. And we've talked about, for example, how Bruce Schneier takes issue with that, saying the problem with a don't-write-it-down policy is that while writing it down exposes it to discovery, it encourages it to be weak because, if you can't write it down, you're going to choose something easier to remember.

Leo: Not writing it down encourages weakness, yes.

Steve: Yes.

Leo: Right, right.

Steve: Exactly. So and then of course don't share it with anyone is sort of obvious. Then changing it often is the other sort of standard policy is, oh, how long have you had that password? You should change that. And it's like, okay, obviously that's sort of common sense. And then, finally, no reuse of passwords across sites. We have often talked about that it's better to have different passwords for different sites, the vulnerability obviously there being, if some employee at one of those sites went bad, or if a keylogger logged you into one site, it might say, hey, maybe this person - or the employee might say maybe this person is using the same password everywhere else. Let's go see if we can log on with their credentials in other places. So obviously not reusing a password is a good policy.

Leo: You know, I recently started using - and you've talked about this, too. In fact, this is our recommendation is these password wallet programs where you kind of have the best of both worlds. In fact, they'll even generate tough passwords for you, store them. You have one master password which you can remember, so everything's protected. But you have different passwords for every site. So I started using one called - which I love and I recommend - called LastPass. I use it because it's cross-platform. But get this. They have - they've obviously listened to the show. In fact, I'm going to say hello. Because they have two-factor authentication - one with YubiKey, works with YubiKey, they're running YubiKey server; the other with Perfect Paper Passwords.

Steve: No.

Leo: Yes. You can print out exactly what you do, what you recommend, a sheet of paper for your second factor. You put it in your wallet, cross it off. It's as if they were listening to the show and tried to design the perfect password storage system. I just love it.

Steve: I'll check it out.

Leo: LastPass.com. It's free. If you want the pro version it's a buck a month. And I've been using it. And I put it on every browser, on every system - Linux, Mac, Windows, Droid, iPhone, everywhere. It's really great. And they obviously are Steve Gibson fans.

Steve: So having run through what we all agree from, I mean, in fact, passwords were the first three or four episodes of our podcast four and a half years ago...

Leo: Oh, yeah. Oh, yeah, the most important thing, yeah.

Steve: Having run through - and of course this is what most people, you know...

Leo: It's the first line of defense, yeah.

Steve: ...when they're using, well, it's the first issue of security they encounter when they're on the Internet today. No matter what it is - email, any kind of an online account, whatever - that's the way we protect it. So backing away from this for a minute and taking an okay, wait a minute. Now, we're not talking about the listeners of this podcast. We're talking about our moms, or girlfriends, boyfriends, people who are not listening to a security podcast because they're fascinated by the mechanisms and machinery and, I mean, are curious about what can go wrong, but users who just want to use the Internet; someone who wants to be safe, who's aware that there are dangers, but isn't into it for the sake of being into it, but just wants to be okay.

So here we give them all of this criteria. It's like, oh, well, here's what you have to do. And your password's got to be like this, and it's got to be like this, and you have to change it all the time, and you can't use the same one. I mean, at some point they're like, whoa, hold on a second. I can't use - you're telling me I have to have a really fancy password with different upper and lower cases and numbers and letters mixed in. And I can't write it down. And I have to change it often, and I can't use it in multiple places.

And so if we take the contrary position, it's like, okay, what's the likelihood of there being an exploit, of there being a problem with this? And what Cormac does in his paper is he challenges this advice, not saying, oh, yes, it wouldn't be wonderful if everyone did this, but saying what's the cost of doing it? And the point is the cost is not nothing. If I were to try to explain that to Mom, the feedback I'd get from her as she rolls her eyes is, "Honey..."

Leo: Get real.

Steve: Well, "I'm just going to unplug the computer."

Leo: Right, right.

Steve: And so really, if we look at changing it often, okay, so what's the risk? The risk is that somewhere far in the past our password would have been captured, but it wouldn't have been used until now. So the not changing it often creates a window of opportunity. But if the password is captured and immediately used, which is probably more likely, then changing your password often provides you no benefit. Right?

Leo: Okay. Let me think about that.

Steve: Because it would only be if you changed it, like, every few minutes...

Leo: Right.

Steve: ...that someone would have to fit within a very small window in order to exploit the fact that you had had the same password. So again, the changing it often, the argument against that is that most times the password is going to be captured and probably used quickly. So it doesn't really matter how long you've had the same password. The only place where that would matter would be if a year ago the password were captured and it hadn't been used until now. So that changing it anytime in that year would have thwarted the attack.

So you could say, okay, that's dumb. I mean, changing it often is, first of all, a real pain because if you just got comfortable with - it's like when I lose one of my credit cards because of online fraud, it's like, oh, I had just memorized the darn thing, and now I've got to go memorize it again. So changing your password is very expensive from a user argument, from a user cost, and it's not really clear. It's like should you? Yes. What happens if you don't? Probably not a big problem because the nature of the attack is not using real old passwords. That just probably doesn't happen.

Leo: Right.

Steve: Now, how about the no reuse of passwords across sites? So we talked about what the cost there is, or the exploit is, some sort of cross-site abuse where something sees your logon credentials, something or someone, a keylogger or malware or a trojan or something, or an employee at a site that's a bad employee at a site sees your credentials and then specifically tries to reuse them on other sites. Could it happen? Yes? How likely is it? One of the problems, and it's a really good point that Cormac brings up, is we don't know the answer to these things. We don't really - we in the security community don't have real quantified research about the nature, the size of the risk.

Leo: That's interesting. We're just assuming empirically.

Steve: Theoretically, see, this could happen. Oh, no. It's like, no one can argue that it could happen. But the beautiful, like, rational response to, like, if someone were trying to, like, push too far is - and this is your response, Leo - well, okay. How likely is that?

Leo: Right. Well, you have to have that information to weigh your response; right?

Steve: Yeah, you absolutely do, in order to know whether the cost of following the advice is worth the expense of not. Now, he raises another really good point in this whole domain of phishing. And I've talked often about how really annoyed I am that Mom has to deal with URLs.

Leo: Right.

Steve: And of course phishing is really, if you think about it, really tough to train a non-computer user about. First of all, we have to tell them, okay, IP numbers in the URL, those are probably bad. So if you click on something, and it's 29.243.16.71, you know, to make up a random number, it's like, oh, you know, you can't tell anything about where you just went. So that's scary. That's probably bad. Except that they might see 192.168 dot something dot something. Their local network IP could appear in various contexts when they're talking to their local machine or another machine on the LAN. So then it's not bad. So that's confusing.

Then we have the problem of a link, for example in email, that says www.paypal.com, but that's an HREF in HTML where it's actually where the URL associated with what's visible, you're seeing www.paypal.com as a clickable link, but the HREF is www.drevil.com. So now we have to say to them, oh, well, you can't trust what it says, what the link says. That's like, oh, what? Well, how can I ever click on anything? It's like, well, no, you can't. Just don't.

And then there's the problem of www.paypa1.com. Looks like PayPal to a cursory view. But it's a number one. And so we have to explain to them, okay, that's not the same. So look carefully, make sure every letter is what you expect, not something that looks similar. Oh, and by the way, www.paypal.ru, that's bad, too. You know, there is no PayPal in Russia. You can pretty much guarantee that you're going to have a bad experience if you go to PayPal.ru. So then we have to explain to them that the com is important. But then the next thing over, the second level domain name, is really where you're going. Except there's Amazon.co.uk. That's good. But BofA.co.uk, oh, that's bad. So, I mean, think about how incredibly confusing the knowledge of how to parse a URL, I mean, we all, the listeners of this podcast, take it for granted. We know how to read this. Oh, and another favorite of mine is if we tell them that you have to read from the right to the left because of course URLs, you know, we have com as the top level domain, and then the second level domain is where you're going. So, for example, we explain that www.paypal.com.drevil.com...

Leo: Is not the same.

Steve: That's bad, too, because that's really DrEvil.com, and it's a machine down the tree from him.

Leo: But you're right, we shouldn't have to have URLs. In fact, Tim Berners-Lee said I never expected anybody to be using URLs. This was for machines, not humans.

Steve: And then - I'll wrap this up. Because if then they're presented with www.drevil.com/www.paypal.com, now they're thinking, oh, good.

Leo: It's fine.

Steve: It's fine because it's PayPal.com on the right. But no, that's behind a slash, so that's a directory of DrEvil.com, and you're in trouble again. So, you know...

Leo: It's not commonly understood. You and I and everybody listening to the show knows it. But it's not common.

Steve: And I'm exhausted from just giving those examples.

Leo: I know.

Steve: I mean, there's so many ways this can be wrong. And we're trying to tell users, oh, check to make sure where you are. You cannot, I mean...

Leo: Yeah, you can't.

Steve: ...it's not reasonable to tell where you are. And then I love the point that he makes about SSL certificates, which is virtually 100 - and I know I just said the word "virtually." I've been told that I use the word too much. It's like, okay, that's the one I need right here. Virtually 100 percent of certificate errors are false positives. That is to say, if you think about...

Leo: What?

Steve: First of all, phishing sites don't use certificates. So the only time you can get a certificate error is if there's a certificate in play, and something's wrong. You don't get a certificate error on a non-SSL page. And phishing sites just don't bother with HTTPS. All the studies have shown that users don't look. Users don't understand the difference between what's the content of the page and what's on the browser window dressing, the so-called "chrome" of the browser. Users don't understand that a lock showing on the page is different from a lock down in the tray.

Leo: No, yeah.

Steve: Or in the URL.

Leo: I don't even know how you'd explain that to somebody.

Steve: Exactly. Again, my model is my mom, like the person who wants to be poking around on the 'Net, and I want to keep her safe. And she's already signed off after, like, a minute of this. And the other thing is, it's funny because, I mean, when I approach somebody who is a neophyte, and they say to me, they ask me, okay, well, what do I need to do to be safe?

Leo: I don't know.

Steve: You know? There isn't an easy answer. The fact that I don't even know how to answer that question...

Leo: Wise up. But that's not a good answer; you know?

Steve: No, because here we are four and a half years into this, and we're still talking about new stuff that's coming along. So on the SSL certificate, just to wrap that up, the point that Cormac makes very, I mean, robustly is that the only time you see certificate warnings is when, for example, a certificate is expired. Remember, not long ago GRC's certificate expired. I was at Starbucks, and someone sent me email saying, "Hey, Steve, by the way, I hope you were...." And in fact I was spending, I was going to spend a whole day working offsite. And it's like I had to run home and solve the problem because my certificate expired. It just caught me unaware. And I've talked about how when I have seen errors, I've gone in and pursued them, and sure enough, without exception, the certificate expired a day or two before. And I know they're running around, scrambling, trying to get their new certificate issued.

So over time users see these sorts of problems, like certificate errors, and they - I still sold SpinRite with an expired certificate because people had gotten used to it and thought, oh, well, maybe they checked the certificate themselves and saw that it had expired at midnight, four hours before. Or maybe they're just already used to false positive certificate errors. But for whatever reason, studies have shown people ignore them. And that in fact they are right to do so. They're behaving rationally when they do that.

Leo: Because 99 percent of them are false positives.

Steve: .999, I think, yes. And the point is that bad sites, phishing sites, just don't use SSL, so they don't have a problem. Or in the rare...

Leo: That's a good point, too, right. You don't see a certificate error.

Steve: Exactly. You can't get a certificate error if you're not even trying to use one. And the flipside is, in the rare case that they have gone to the trouble of issuing certificates, they've also gone to the same trouble to make sure everything's correct. So for them, the correctness of their certificate is their whole life. I mean, this is all part of the spoof that they're trying to pull. For me, I've had certificates for years. It's sort of an annoyance that I have to renew them every couple years. So I'm not thinking about it the way somebody who's focused on valid certificate spoofing is thinking about it. For them, they're going to make sure nothing generates an error because that's all part of their campaign.

So what happens is, with all of this - for example, in the cat and mouse game with phishing, the original phishing hacks were numerical. So we told users, oh, don't trust numbers. Then, okay, people started - the bad guys evolved to lookalike names, PayPa1.com. Now we tell users, oh, you've got to look at, you know, numbers are still bad, but now look, make sure that every character is correct. And then there was a next level of escalation. And we ran through all the wacky ways that you can obfuscate a URL that's visible to confuse users. And these are people who have actually somehow been convinced that this is something they have to worry about.

And so the argument is, what's the cost of just ignoring all of this? The fact is the written policies of all the banks are you're indemnified. If you notify us within a couple days of some problem, of you becoming aware of the problem, your maximum liability is $50, or zero. Policies vary. But in general, because the bank or whatever financial institution is wanting to encourage this Internet use because it's good for them, it lowers their costs, it allows them to streamline and automate and outsource and all that, they're wanting to say, okay, we'll take responsibility for there being a problem. I mean, I've never paid anything when my credit card has leaked out onto the Internet. I get a call. They say, Steve, were you in a French health spa yesterday?

Leo: I get that call a lot.

Steve: And it's like, uh, no.

Leo: No.

Steve: Wasn't me. They go, okay, fine. We're going to cancel this card, and we'll send you another one in the mail.

Leo: Get this one. Jennifer calls me - Jennifer calls me every few weeks saying QVC is on the line again. They say we bought $800 worth of crap, and they're shipping it to Southern California. And they give the same credit card number every time. And it's one we haven't had in years. It was canceled years ago. Somebody continues to use it with their address and our phone number. But the funny thing is, QVC, I don't know why, but they ship them the goods. It's like, I'm not liable. I haven't used that credit card in years.

Steve: Wow. That's nuts.

Leo: But I love it when I get the call because then I, you know, it's like, well, at least they're paying attention, I guess. But why are they shipping this stuff?

Steve: So what we have is a mess. And with the users being protected from the exploitation of their identity. Now, I would argue that identity theft is something where we've all heard the horror stories of what happens when your identity actually gets stolen, and it's a big problem. But even there, if you do the math, if you look at - apparently there are 180 million adult users of the Internet in the United States. And if you just on the back of a napkin sketch out how much time out of everyone's day goes into scanning URLs and fussing around with passwords per site and password rules and all of this overhead versus what's the expense to the user of not doing so, Cormac makes a compelling case that all of this is just nonsense.

Leo: Yeah. But you've got to do something.

Steve: Well, and it's very clear that LastPass and what you're doing makes sense for you.

Leo: Yeah.

Steve: I'm looking forward to checking it out myself because it sounds like a beautiful solution, one I can understand. And all of our listeners understand this. Mom doesn't. You know? That's a threshold that is too high for her. And in fact I recognize it when I talk to somebody who wants my advice and isn't a Security Now! listener or a candidate, they want, like, where's the tradeoff? And the perfect question for them to pose back to me is, well, how likely is that?

Leo: Yes.

Steve: I mean, that stops me cold because all I have is the absolute knowledge that it's possible. But I have no idea how likely it is. And one of the things that occurred to me as I was reading this that Cormac did not discuss is one thing that we're lacking is positive feedback when something we do saves us.

Leo: Oh. Like that was a good thing to do, yeah.

Steve: Yes. We never get that.

Leo: That's a good point.

Steve: We don't - we're not - we don't get awarded for links we don't click in email. We just know we can't click those. But imagine if you actually knew that, had you clicked it, you would have been in bad shape, well, that would positively encourage you. Similarly...

Leo: Nice job, Leo. You just avoided getting phished. Yeah, yeah.

Steve: Reality just split. Leo clicks the link; Leo doesn't click the link. Look at the world if Leo had clicked the link. Oh, my god.

Leo: Right, right.

Steve: And I'm running with NoScript, so I'm blithely jumping around from site to site. But nothing is telling me, whooo, boy, you just avoided a bad one right there.

Leo: You've got to have some positive reinforcement. That's key, yeah.

Steve: So you don't know what the scripts you don't execute would have done to you. And so one of the problems is that we know listeners of the podcast whose shields are up, who are protected, who are using complex passwords, who do look at URLs, who do scrutinize the links in the bottom, these bad things are not happening to us. But still we don't - there is no system that tells us what horrors we avoided by behaving ourselves well. So one of the things that is missing, I think, is positive feedback for our good behavior. I mean, we're still going to be on good behavior because we understand the consequences.

Leo: Right, right.

Steve: But I do have a friend who is long-winded about answering questions. And whereas I sort of...

Leo: I know your friend. I think I've had dinner with him.

Steve: Yes, you have.

Leo: You didn't have to say more than that.

Steve: And I've watched people ask him this sort of question. Well, you know, what do I really need to do? And half an hour later, when they start to snore, he's like, well, okay, I'll finish this after you're awake. And the fact is, it's just not practical to explain to most people. But the question is why? It's because it isn't worth it. And most users get that intuitively. We like security for its own sake, because it's fun, it's interesting, it's got mechanisms, it's got good guys and bad guys. And we do know, we're very conscious of what could happen. We hear about them, these actual things happening to people all the time, too.

But most users make a different, purely economic-based - for us it's a hobby. Most people don't want to mess with this. They just want to get on with their life. They make an economic judgment which says, okay, I know that some people, I've even had friends that have gotten viruses. And they don't know what they did; I don't know what they did. This all makes me very uncomfortable. But I'm just going to push on and hope for the best because I asked somebody once what I should do, and I just glazed over because I couldn't understand half of what he was saying.

Leo: But we need simple - we need maybe - I don't know who's going to do this, or even if it's doable. But we need some sort of quick, easy, simple instructions. I endeavor to do that on the radio show because I can't give them two-hour instructions.

Steve: Well, and Cormac makes the point, and this is what I have done, is he talks about prioritizing. He says, if you go to US-CERT and look at their rules for, like, proper security, it's pages of dos and don'ts. But, for example, my number one thing is do not click on links in spam. Number one. So if you ignored everything else, do not click on links in spam. I would argue that's probably the worst thing you can do. And so then if you created a hierarchy - and so that's a simple, clean, clear rule. Now, then the question is, well, what about links from Aunt Sarah? Oh. Well...

Leo: You want to hear my rules? This is what I do on the radio show because you have to codify it. And people get mad sometimes because I don't give them shades of gray because you can't give them shades of gray. You have to say, do these five things. To me, number one is run Windows Update automatically, religiously. Because even if you continue to click links, if you're not vulnerable to the exploits, you're going to be protected. So number one, Windows Update. Number two, don't click links in email or in Instant Messenger. Number three, don't open email attachments. That's become lower down on the thing, on the list because that's no longer a common vector of viruses. It used to be number one, email attachments, but less so now.

Steve: Right.

Leo: But I extend that now to say don't - and by the way, the true, as you know, the true rule is do not open executable attachments. But of course most people can't tell.

Steve: Right.

Leo: So you can't say don't open executable attachments. You just say no attachments. I also say don't accept files from strangers, and that may be on Facebook, from peer-to-peer, you know, links and files are really the deadly vectors these days; right? That's where the viruses get in. And I think those are simple enough that people can remember. You know, I should add make good passwords and stuff like that. But those are simple enough that I think people can remember them and act on them. Would you add anything to that list?

Steve: I think, no, I think you're right. I think in terms of a hierarchy, I think that that's the minimal behavior for people being safe. And everything beyond it, the content of this podcast for the last four and a half years, are looking more closely, dissecting threats, understanding them. But I liked this for our end-of-the-year topic because I really do think that there's a very good point, and that is that, arguably, that comeback of, well, how likely is that, it's probably not that likely.

Now, arguably, links in spam, ooh, you don't want to go to - you don't want the universe to fork and take you down that road. Clearly wrong. Phishing attacks, well, we know they happen. But then again, it's easy to get over-paranoid, that is, am I happy when I lose my credit card, when it gets loose because I've used something other than PayPal? No. I'm not happy. But I'm protected. I get another one. Life goes on. And there's some cost to me. But I was pretty much indemnified for, well, I was completely indemnified for that. And so that's the case with most of this kind of online fraud, is users are safe.

Now, losing your identity, getting your machine all mucked up with stuff, you know, that costs you time and trouble and annoyance. And it's happened to most of the people who are neophytes. I've looked at their machine. I've tried to figure out what they did. Typically they clicked on a link in email. That did them in. So I really think that's the big bull's-eye, and everything else is interesting, theoretical, worth discussing.

Leo: We're not saying - and somebody in the chatroom said, Hartwell said, "Well, I guess this is the last Security Now! ever." We're not saying that you don't talk about it. People who listen to this show want to know all the other stuff. We're talking about what do you tell Mom.

Steve: Yes. We're discussing the science of Internet security.

Leo: On the show, yeah, yeah.

Steve: The science and the technology and the practice. And, well, and it's from that that we're able to distill the most important things, and that inherently means there's going to be some least important things, some things that are less likely to happen. And certainly our listeners want to know about parsing a URL and being not caught out by something that might be strange. Most people are just like, oh, don't confuse me with all that. I just want to buy my doughnuts and go on.

Leo: [Laughing] I love it.

Steve: So the rational rejection of security advice is...

Leo: Sometimes it is rational.

Steve: It is rational. And it is arguably in many users' best interests. See, the other thing, Leo, is for us, listeners of this podcast, these things are not expensive. I do look at the URL.

Leo: Right, right.

Steve: That's part of my experience of using the 'Net is looking at the URL, checking the URL of a link that I'm hovering over before I click on it. It's inexpensive for me to do that. It is not inexpensive for Mom to do that because she doesn't really understand it. And that's the problem. We're giving people rules to follow. We make the rules. We understand, you, I and our listeners understand why and where they came from. Instead, we're imposing conduct on people that just sort of - they don't really understand where it came from, why they're being asked to do that. Well, what is this URL? So it just makes them anxious and uncomfortable. It makes them itchy, and they're not happy. And we might as well have people who are probably going to be okay, and happy, than maybe not that much safer anyway, and miserable.

Leo: Steve, I think this is a great episode to hand around to your friends and family. And maybe someday we'll write a little pamphlet. There must be something like that out there that's just the basics, what you should do, what you need to know, how to protect yourself in 99 percent of the cases. The other 1 percent, you should be listening to Security Now!.

GRC.com's the website. You can go there right now and get a 16KB version of this show for the bandwidth impaired. Steve also pays to get transcripts done. Elaine Farris writes those up and so you can read along as you listen. He also has a whole bunch of great free programs, security programs there, and the flagship of the operation, the great SpinRite, a must-have hard drive maintenance and recovery utility. If you don't own SpinRite, go get it: GRC.com. Happy New Year, Steve.

Steve: Happy New Year to you. We're plowing into 2010, and I'm sure we're going to have lots of fun and adventures for our listeners.

Leo: 2010. You know that's the year we make contact.

Steve: I'm ready.

Leo: Yeah, we'll see.

Steve: I'm way more than ready.

Leo: It's about time.

Steve: Yes.

Leo: All right, Steve. We'll see you next time on Security Now!.

Steve: Thanks, Leo.