Personal Password Policy - Part 2

Description: Our previous episode (#4), which discussed personal password policies, generated so much great listener feedback, thoughts, ideas, and reminders about things we didn't mention, that we decided to wrap up this important topic with a final episode to share listeners' ideas and to clarify some things we left unsaid.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-005.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-005-lq.mp3

Leo Laporte: This is Security Now! with Steve Gibson, Episode 5, for September 15, 2005. And here we are in Toronto.

Steve Gibson: Yeah, for the first time together, doing a Security Now! podcast.

Leo: Live.

Steve: Absolutely, together, face to face instead of over some wacky VoIP solution that we're still trying to nail down.

Leo: This is much better, I think. It's a good way to do it. So we got a lot of response - we've gotten response on all of our podcasts so far. But the last one, Passwords, got a lot of response. We thought we'd address that.

Steve: I think part of the reason, of course, is that we were soliciting response. We didn't intend, really, to make it a two-part podcast, but that's what we decided to do. We're going to do Part 2 now of Personal Password Policies, based on a lot of the feedback - or at least, you know, triggered by a lot of the feedback that we received because, having asked for feedback, boy, you know, we got it.

Leo: And most of it was positive; right? Was there anybody who said we had a bad idea?

Steve: One person made a very good point, and that was that, if you - you remember that we talked about the idea of taking a domain name and, like, munging it, using your personal hashing algorithm to swap the letters around and do things. Well, he pointed out that, if you did that in an obvious way, somebody could reverse engineer your personal password policy and then go hunting for other sites where you might have used the same policy on a different site. I mean, it's a point that is certainly worth making, that is, if you were going to use this approach to create a special password on a per-domain basis, you'd want to do something where looking at the result it wasn't obvious what the domain was. So...

Leo: I've got to go back to the drawing board.

Steve: Exactly, so be clever. Now...

Leo: Well, as an example, just so people understand what we're talking about, if you had a password for Google.com, you might intersperse it with your Social Security number, so it would be g5o5, that kind of thing. That would be an awfully transparent way to do it, however.

Steve: Right. So you'd like to have something where you're a little more clever about that. Another person made the very good point that we didn't - I didn't really fully answer your question, or correctly answer it, to, like, what is a good password? Because we immediately launched off on the whole dictionary attack idea. But the other attack on a password is the so-called "brute force method," where you just start with A, then B, then C. And then when you run through Z, you go, okay, he didn't use a one-letter password, how about the two-letter passwords - AA, AB, AC, AD and so forth. So the point is that password length is the other thing that is certainly important. You don't want a too-short of a password because then it's possible to try them all.

Leo: So what would you say would be a good starting point? Eight? 12?

Steve: Well, the strength goes up quickly. For example, if you have lowercase alpha and uppercase alpha and number signs, just for example, so you've got 26 lowercase, 26 uppercase, and 10. So that's, what, 62 symbols in each character position. So each character position goes up by a factor of 62.

Leo: So there's 62 possibilities for a one-character password, and 62 squared for a two-character password, or 62 cubed for three - well, you could see very quickly that even eight would be enough if you used all of those different possibilities.

Steve: Yeah. Now, some sites, of course, will - they're not case-sensitive, so you wouldn't get credit for using uppercase, and you wouldn't get any sensitivity. But, I mean, I guess it's a function of application.

The other thing that we touched on last week that I think I wanted to come back to is this notion of the importance, or the idea, of varying levels of security. For example, you might argue that you only want to use the password that you use for PayPal on PayPal, and on your banking site, only there, and never be tempted to use it again. A number of people came up with sort of acronym-based approaches, where they're lyrics to their favorite song or some verse that they like. Or some guy was saying, well, how about like if I was on my banking site, then I'd think of the phrase "Show me the money," and I would use some sort of password based on that. So the idea of, like, using something memorable that's easy for them to memorize. We heard that from a lot of people.

Leo: Difficult, though, if you have dozens of these sites. I mean, if you go to your investment site and you hum "We're in the money," and you go to your bank site and you say, "Show me the money," I mean, you'll run out quickly, and you could easily get confused.

Steve: You can get yourself tangled up pretty easily, too. But I guess the - and another approach that actually you and I talked about in something we did before, it may have been on TechTV or something, is the idea of using the keyboard as your - sort of your crypto device. Look at a word on the keyboard, and then skew the key presses like up and over, to the row above and to the left. And so if any letters fall in the top row of alphabetic, they go into the numbers column, and you pretty quickly end up with something which visually you'd never guess what it was. If someone were trying to crack it, you know, and they thought this might be what you were doing, they might look at the keyboard and try to figure out what way you went. But you could do other things like, you know, go left, up left for the first character, up right for the second one, down left, I mean you could get some - you know, again, that's sort of a variation on a personal algorithm that is very unlikely to be cracked.

Leo: But I guess we should point out that ultimately only something that's completely random is going to be completely secure. The less random it is, the more likely it is to be cracked.

Steve: That's the perfect parameter. We know that something that's random is the least likely to be, you

know, to appear on the keyboard, in a dictionary, or anywhere else. And so you take the randomness times the length. And that really gives you your raw sense of strength.

Now, the other question is the issue of is it necessary, really, to have per-site passwords? I mean, you know, you and I confessed last week that we've got, like, a collection of passwords that we sort of use and re-use. And so sometimes when I'm on a site that wants me to log on - I hate these ecommerce sites where you have to create an account. Because, like, I don't want to create an account. I just want to buy this. I'm never coming back. But no, no, you've got to join. So, you know, so I'll frequently be going, okay, now, what one of my little collection of passwords that I re-use did I use here? And hopefully the site is patient while I guess and doesn't time out on me.

Leo: I do the same exact thing. And you'll enter passwords five or six times, trying all the variations of the password, yeah.

Steve: So I'm not clear that it's necessary. I would say, don't reuse your critical site passwords that are based on ecommerce or banking or check management or stock portfolio stuff. But, you know, frankly, I think you could relax. Because really, what would the attack be if someone at some arbitrary site, you know, figured out that you used this password, and this was your email address. Well, they'd have to go to, you know, every other site on the planet to get a collision of your use of the same password and so forth. So I think it's very unlikely.

Leo: Another thing we didn't address, but I do, is also vary the log-in. If you always use your name as the log-in, that's pretty easy to guess. But if you have kind of nonstandard log-ins, those are going to be difficult to guess. And then combine those with your password, it's going to be a pretty tough...

Steve: If you have the opportunity to do that, that's a perfect idea. What I'm seeing more and more is the use of email addresses as the username. So there you'd be stuck having to create some temporary accounts which, you know, we've all done when we want to go somewhere that we're not going to be tracked down. But maybe then the approach is, the variation on the log-in name, is to have some and maintain some throwaway email accounts to use, you know, for random places you go that you're never going to come back to.

Leo: Here's a good trick Kevin Rose taught me. Google allows you to take your Google address - mine is Laporte@gmail.com - and append a plus and then any arbitrary string of, I think, eight to 10 characters to it. So if I do Laporte+security@gmail.com, it still will go to my Laporte account.

Steve: So it creates, like, mailboxes within your master account.

Leo: And you can then filter on it, whatever. But you essentially have a very, very large number of email addresses that all go to the same account. So you could use it for that purpose. For instance, I could have as my New York Times log-in Laporte+nytimes@gmail.com, and that would be unique to that log-in.

Steve: As long as it's @gmail.com. Yeah, it's not generally the case that that works, unfortunately.

Leo: It's only gmail, let's get that right.

Steve: The other thing that we got many questions about is, what about the password managers that are built into some web browsers? Because clearly, you know, I guess the Mozilla Firefox browser has a built-in password management facility. And I'm a little nervous about that only because it happens to be built into a communicating application. The idea of a third-party password manager makes me feel safer than a password manager built into a browser.

Leo: There are some like RoboForm that is a third party, but integrates with a browser. Would you say

that would be more secure than using the one that's built into the browser?

Steve: I would say that's more secure because you can - it's easily possible to envision an attack against a browser's built-in password manager itself, where you go to a site that takes advantage of a scripting vulnerability to get into the browser, and what this particular site has chosen to do today is suck out all the passwords that anyone visiting it has. So to me, I mean, to me that seems like an Achilles heel. I mean, it's tempting as all get-out because, hey, look, it's built in, I'm at a website, my web browser knows what website I'm at. I mean, what a cool idea.

Leo: I think we all use it. I mean, I kind of rely on Mozilla Firefox's password memory.

Steve: So again, maybe that's the place where you make a conscious decision, I'm not going to do that on my critical sites.

Leo: And most banking sites, for instance, won't let you do that. Most sites somehow disable that capability. So, for instance, my banks I cannot - I can't memorize the password. And the other thing you don't know is how cryptographically secure those password stores are. I don't know what they're - they may be in plain text.

Steve: We would certainly have to presume that whoever it was who was creating a password storage facility for the browser took advantage of, you know, state-of-the-art crypto. And, I mean, crypto is so strong now. As long as there's no mistakes made in the implementation of it, then you're really safe. Now, the flipside of that is, okay, what about if malware got into your computer and said, oh, I'm going to suck out all of the passwords in this browser? Well, I thought about that for a while. But my feeling is, well, if malware gets into your computer, you're pretty much hosed anyway.

Leo: They can record your keystrokes.

Steve: Exactly. A keystroke logger to watch you type in a 16-character credit card number, do the little Mod 9 thing to verify that it is a valid credit card number, and then send to the mothership, wherever, you know, everything you've typed in for the hundred keystrokes before and the hundred keystrokes later, and they've probably got the entire log-on and ecommerce data for you.

Leo: This is a complete digression, but is that what they do? They do a Mod 9 on the number?

Steve: That's what I would do.

Leo: We don't know what they do exactly.

Steve: Well, for example, you know, I wrote my own site's ecommerce system from scratch. And so it's well known that if you add up all the digits, it is a Mod 9 function. And what that does is it catches digit transposition. It won't catch them if you swap them, they're two digits apart, but adjacent digit transposition. So that means that technically only one out of every nine credit card numbers is valid. So it has a one in nine chance of catching an invalid one.

Leo: That's nice to know.

Steve: So were I a bad guy writing, you know, a let's suck out, you know, I mean, let's really do some nasty malware, I'd do a keystroke logger because that way you're upstream of everything. And I just have a big ring buffer of everything that the guy is typing in. And when 16 characters have been typed in, and they match the Mod 9, the chances are he's just entered a credit card number into his machine. Well, he's entered a bunch of other information first, and he's probably going to enter some more information later. So if I had

a big ring buffer, I'd have the last thousand things he typed, keyed by and triggered by a valid credit card number being typed in...

Leo: And catch almost all the credit card numbers. Now, this raises another issue for security pros, is that by taking about these things, in fact, you've just told somebody a pretty good technique. Do you presume that they already know these?

Steve: I hope so.

Leo: It's kind of difficult to talk about security and not reveal, sometimes, tricks that a bad guy could use. At least any bad guy listening to this is going to have some better ideas about how to try to steal passwords.

I want to give a little plug for OSX because it has a built-in password manager called Keychain and Keychain Access that is cryptographically secure. It's unlocked by default by you logging into your account, and it does remember passwords. It actually has a password assistant that allows you to choose good passwords. It will generate good passwords for you. And it's the one that does the fill-in in the browser. So it's separate from the browser.

Steve: Right, well, that sounds perfect. And speaking of that, we did get a bunch of people wrote in with their favorite password tools. We got about 15 of them. I read through all the email and all the submissions that I received. You may have received...

Leo: I forwarded them all to you.

Steve: Okay. So in the notes on TWiT.tv we'll put the URLs of everything that we've been sent. These are not our recommendations. But it's our listeners' recommendations. And, you know, there's freeware, there's open source, there's shareware. Some of the things are Palm OS or Pocket PC. They integrate with your PC or your Mac so you're able - in fact, I was surprised by how many people are carrying USB dongles around with their passwords stored in them. So, I mean, there are people listening to this who are really taking - are already taking this really seriously.

Leo: That's a good thing, yeah. These will show up in the show notes on the website, as you mentioned. But also they are part of the RSS feed. So if you use an RSS reader or a podcast client that can see the full RSS feed, you'll have all the links in there, as well, for clickable purposes. I've been doing that for a little while. It's actually a great way. iTunes doesn't do it, but for a lot of the other podcast clients. You don't use any of these, though, yourself.

Steve: No, I don't. I've got my little asynchronous Palm Pilot, and I do - I am happy that I have a Palm 5 now because they finally took the limit off of how big the notepads could be. There used to be, I think it was a 4K limit. And I was always hitting the end of that. And so I have the Palm. Actually I have two: one that I travel with that is my eBook reader. That has no personally sensitive information in it at all. It's got eBooks and TV programs and things. And then the other one sits right by my side. And again, I don't dock it, and it does not touch my computers because I don't want anything to crawl into it. But that's sort of my offline reminder of which one of my collection of passwords I used on a particular day, you know, whatever mood I was in.

Leo: Yeah, essentially I do a similar thing, only I keep it on the computer, and it's a notebook of all of my passwords and all the sites I've used. And if I don't put them in there, heaven help me because I'll never remember. It's hopeless. Anything else you want to add to the subject?

Steve: No, I'm just glad we spent two podcasts talking about this. The reaction - we did get a lot of mail from people who loved the domain algorithm idea, who basically indicated that we've achieved our goal here, which is to get people to stop and think about this for minute, because it's the kind of thing the importance of which sort of creeps up on you. You know, the first time you log in, you probably don't do the right thing. Well, logging in to online stuff is in everyone's future from now on out. And so if you haven't already given it

time, lots of people who are listening to this already have because, you know, we probably attract that kind of crowd. But for those of you who haven't, sit down, figure out how you want to do it, and take it seriously because passwords and needing to come up with them somehow, one way or another, and manage them is in all of our futures.

Leo: Oh, it's my hope that people will pass these along to their friends and family and share the ideas, at least, if they don't want to share the podcast itself.

We are going to make the podcasts available on a CD. We're trying to figure out - I think the best way to do this, and we'd love to get your input on it, is to not put out an audio CD because we'd only be able to put two or three podcasts, or four maybe, on one audio CD, but to put out an MP3 CD that could contain, you know, dozens of them, and so have a real library on there. So that's what we're probably looking at. But if you have some input, we'd love to hear from you. And of course the website for Steve's Security Now! podcast is GRC.com/securitynow.htm. And he always puts more information up there.

We'll be back next week. We don't know what we're going to talk about at this point. Often it's topical, timed to some big announcement. And sometimes it's just educational. But I hope you'll come back every Thursday. You have a final word?

Steve: I was just going to say that, at the bottom of that page, the list of things we're going to be talking about is growing. I've got about 25 of them now. So we won't be running out anytime soon.

Leo: Guess we'd better do another podcast. Our thanks to AOL Radio at aolmusic.com for providing the bandwidth for this podcast. It makes it possible for us to do this for free and can get everybody who wants a copy to get their own copy. They do a great job for us. Thank you, AOL Radio. And an invitation to visit This Week in Tech at TWiT.tv for more information about this podcast, This Week in Tech, and all of our other productions.

I'm Leo Laporte for Steve Gibson. Thanks for joining us for Security Now!. We'll see you next week.