PayPal Security Key

Description: Steve and Leo talk with Michael Vergara, PayPal's Director of Account Protections, to learn everything they can about the PayPal security key effort and its probable future.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-103.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-103-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 103 for August 2, 2007: PayPal Security Key.

It's time for Security Now! Episode 103. Hard to believe. We're just chugging along here. Steve Gibson...

Steve Gibson: Next week...

Leo: ...from his fortress of security. Next week what?

Steve: Next week, Leo, two years.

Leo: Oh, really?

Steve: 104 episodes, that's two times 52.

Leo: Makes it easy if you don't miss an episode.

Steve: Yeah, I love it.

Leo: You're good at this. We never even took Christmas off or anything?

Steve: Nope.

Leo: That's amazing.

Steve: Nope. New Year's, even when you're out cruising on the water doing geek cruises...

Leo: That's right. We get ahead just for those...

Steve: ...and Vancouver.

Leo: You're good, Steve. So...

Steve: Even when my home is fumigated toward the end of this month, we're going to not miss a beat.

Leo: Are they going to tent your house?

Steve: Yeah, finally, the entire complex. It's 32 years old, and it's never been fumigated. So it's time to kill off all those little wood eaters.

Leo: Well, I'm going to just mention because you won't, because you're a shrinking violet, but this is happening because of you, Steve. You actually actively lobbied the Homeowners' Association. They needed to pass this assessment or it wouldn't happen. And you made a DVD.

Steve: It's true, it's true.

Leo: A campaign DVD.

Steve: We made five - it's my first experience creating a manufactured, you know, a glass master pressed DVD.

Leo: Well, how many did you have to make?

Steve: 500. And we found a company that could do it in four days. So, I mean, literally local, here in Tustin, Southern California.

Leo: So did you make a little film that says "Why we need to tent"?

Steve: Oh, it was great. I have a crystal logo, Homebrew, with little, you know, the little home moniker that I use.

Leo: [Indiscernible].

Steve: And so basically it was an interview of everyone on the board, explaining everything that was needed.

Leo: Oh, that's great.

Steve: We ended up, I mean, no one believed it was possible. But you're right, I spent about the last four months doing little else other than marketing this thing, you know, marketing the assessment. And we got 146 households out of 309 agreed to be assessed $25,700 each, that is, for the full 309, so we're raising...

Leo: That's why you had to lobby. That's a big commitment.

Steve: That's a big deal. But I'm so impressed that our community understood the need for this, and so it worked.

Leo: So we're going to talk in a little bit to Michael Vergara. He is responsible for security at PayPal, and I guess at eBay, too, and is the guy we can thank for the new dongle that we've been talking about, this little identity protection unit that gives you every 30 seconds a new log-in number.

Steve: Right. Oh, it's neat because PayPal somehow found out about our mentioning the security key...

Leo: Somehow? Because they got a thousand orders, probably.

Steve: Well, I hope more than a thousand because, I mean, we've had a lot of questions that came up. And so we're going to get Michael on the line here - as you said, he's in charge of this aspect of PayPal security - to answer the questions that our listeners have asked.

Leo: That's really - that's great. And I think our listeners, like me, are just excited about trying it out because we completely coincidentally just completed this two-part piece on authentication. And I think they were very curious to try this out. So it was perfect timing. It's only $5. We'll talk about how you can get it and how it works in just a little bit.

Steve, any errata, addenda, letters, anything before we get to Michael?

Steve: Yeah, I've got a couple things. One thing I thought was really interesting that I discovered, and I have an interesting SpinRite story from a very computer repair-savvy guy that I thought was interesting. And it highlights something about SpinRite I've never mentioned before, believe it or not.

But the other day I was setting up a new machine. And I needed to do some low-level packet I/O. This is, you know, I have the technology, for example, on our GRC server for emitting packets, sort of very much like the raw socket interface. And in fact I could have used that except it wasn't available back when I was first writing ShieldsUP!. It's the technology ShieldsUP! uses. There's a very well-known library called WinPcap.

Leo: Oh, yeah. Oh, yeah.

Steve: Exactly. I knew you would have heard of it, Leo. So I went there just a couple days ago, and something caught my eye that was very cool. There is now an AirPcap. And there is a company, CACE Technologies, they've got some sort of affiliation with the WinPcap people. I don't know if they bought them or they're a heavy-duty sponsor or what it is, exactly. But the point is that this AirPcap is a USB WiFi gizmo made for sniffing what's in the air. And it's...

Leo: And you're not talking about sulfuric acid. You're talking about the air of your Ethernet, the Internet.

Steve: The idea is that many WiFi cards cannot be put into promiscuous mode or their interfaces don't allow you to get the whole packet, for people who really want to know what's going on. So for $198 you can purchase from this CACE Technologies a freestanding little gizmo. It's like, you know, a little WiFi unit that is a USB interface. So it's freestanding. You can plug it into any system, your laptop or your desktop or whatever, and use it with a whole bunch of free and open source software. They also, for $39.95, have this - they call it the Network Toolkit, which is all of the stuff. I mean, even things like Aircrack that we've talked about, that will hack the passwords that are flying by and now do the high-speed WEP decryption to crack any password or WEP protection in about a minute. They've got another one for an extra hundred dollars, for $298, that will both receive and transmit.

Anyway, I just - I don't know what our listeners' interests are. I immediately ordered one of these things because I - and I'll give a report after I've had a chance to play with it because I just like the idea of, you know, going to Starbucks and easily being able to see what's going on in the air around me. I think it's going to be fun. And so if our listeners...

Leo: Okay, now, we're not saying to do this for any nefarious purpose.

Steve: Oh, no, no, it's just for network monitoring and auditing and making sure that your corporate network is as secure as your IT people think it should be.

Leo: But what it does very much underscore is the risk inherent in using an open access point. Right?

Steve: Oh, yeah. I mean, anyone listening to this podcast, I'm sure that they've heard...

Leo: They know it.

Steve: Many of them, yes. We've pounded that into them over and over and over. And in fact I ran across a question when I was preparing our Q&A for next week that I couldn't fit in, but it was so important I bumped it to the next one, some guy saying, hey, you know, I'm not using WEP and I'm not using WPA, I'm using MAC address filtering, and I turned off the broadcast on my access point, so I'm safe; right?

Leo: Oh, please.

Steve: It's like, no, go back and listen to some more Security Nows, please. Anyway, for people whose curiosity has been piqued, it's www.winpcap.org. Or you just put WinPcap into Google, which is how I remembered where it was, and it's the first link that comes up. And you'll see a little blurb over on the right that talks about AirPcap. And you can follow the links to grab this little toy, which I think is very cool.

Leo: Excellent. Excellent.

Steve: Okay. So getting to my little SpinRite story of the week, Steve Shank has a business. In fact, his motto on the email that he sent was "Keeping clients' computers safe and profitable for over 20 years."

Leo: I love it.

Steve: So he's been doing this as long as SpinRite's been around.

Leo: Long as SpinRite's been around.

Steve: And it's funny because his email, he's an avid listener to Security Now!. He's using Thunderbird to send email. And the subject was "SpinRite Testimonial with a Twist." And he said, I figured I'd let you know what happened to me because it is different from the testimonials you have been reading, and I think it is important for listeners. Also, I think it makes a good testimonial.

A client I've seen only once before calls with catastrophic failure. Windows won't boot, no safe mode, no last good configuration, just constant return to menu asking how to boot. So I made a house call to their office. I watched the process, and it said there was a bad Boot.ini file. So I used the system restore disk to get to the Recovery Console and figured I'd delete the Boot.ini, then rebuild it with Bootcfg/Rebuild, then run Fixboot. These are all MS tools accessible from the Recovery Console. I thought I had at least a 50 percent chance this would work. But the system would not let me change the attributes on the files so I could delete the bad Boot.ini. In fact, I couldn't find the Boot.ini file. In fact, I couldn't get a response from DIR. Yup, no directory even.

So I took the computer back - this guy obviously knows what he's doing. He said, so I took the computer back to my office and ran SpinRite on it. SpinRite said, and I don't remember the message exactly, but this is the gist of it, that the disk was in such bad shape and had so many problems that it thought the disk was on its last legs. SpinRite warned me to get my data off

before running SpinRite, as the exhaustive testing SpinRite does might be the last thing this drive ever does. He says, all the other testimonials you read are from people so happy with your wonderful product and how it saved them. But this message made me feel really good. Your program saw a possible problem and warned me off, saving my data by not running. To me, this indicates a concern for your clients and honesty and integrity which is much more important than the fact that the program works when it can. I do know that SpinRite works, he says, parens, I've used it for many, many years through many versions. Then he opens parens again and says, I used to have to buy multiple licenses to use one on each client computer it worked on. Now thankfully I can get a reasonably priced consultant license, and in my case a very inexpensive upgrade to the consultant license. Then he closes both of his open parens. And he says, and there are situations in which it would have fixed these problems. But here it is warning me not to continue with the program.

Leo: Isn't that interesting. You knew that it would do this, of course, you put it in there.

Steve: Well, actually I don't know whether I said in that message, yes. But what he's referring to is the Smart Data. SpinRite polls the drive's Smart information and interpreted it before it even started and decided that, whoa, things are so bad that this is just not safe to proceed. And so in that case SpinRite brings up a message and says, you know, we'll help you, but things are looking so bad here that before we even start we know this disk is in trouble. You really ought to pull what you can off before you go any further.

Anyway, his message ends by saying that he ended up doing what we suggested and struggling to recover files, did get important files off, and then ended up replacing the guy's hard drive, and actually sold him a new computer because it was time to do that, too, even though that wasn't his first choice.

Leo: So there's a case where Smart Data actually is of value.

Steve: Yes. There's an all-or-nothing flag that Smart is able to bring up that says, I am in serious trouble. And in fact some BIOSes check for that. I know that there are people that have said, hey, my BIOS just told me my drive's about to fail. And that's what the BIOS was doing was turning on the Smart Data and checking the BIOS. Unfortunately, not all of them do that. For example, this customer's BIOS didn't. The drive had to go belly-up first. And what's really sad is that, you know, if anything had been run on this drive before it went belly-up, then that problem could have been found early enough to make the recovery much more easy. So anyway.

Leo: Very, very interesting.

Steve: Interesting spin on SpinRite.

Leo: Before we get to our guest, again, Michael Vergara, any other thoughts, comments, suggestions, corrections?

Steve: I think we've got - we have a long conversation with him, so let's get into it.

Leo: All right. So Michael's on the line with us right now from PayPal's headquarters.

Where is that, Michael? I don't know where that is.

MICHAEL VERGARA: It's in lovely San Jose, California.

Leo: Oh, all right. You're kind of in the eBay building, then.

MICHAEL: Actually eBay has two campuses. There is the South Campus near Campbell. That's where most of eBay is located. And then we're in the North Campus, which is right off 101 and 87, right near San Jose Airport. And a lot of the PayPal people are there.

Leo: Is your job a new job with PayPal, the Director of Account Protection?

MICHAEL: I started about a year ago; so, yeah, I would say it's pretty new, dealing with really the authentication and now verification. So it's dealing with these new, cool devices like Security Key, as well as working on other products and policies we need to have to help reduce the phishing threat that many of our customers face.

Leo: Was that what your mandate was a year ago when you started?

MICHAEL: Yes, really to look into that, how do you create the right policies and products to do that, move it around, and make sure that our customers have both the education as well as products they need to be safe on the Internet.

Steve: So of course this all began when I happily discovered that I could get the Security Key for my existing PayPal account. And essentially we had talked a few weeks before about the whole multifactor authentication thing. And it's like, hey, for $5 I can add this to PayPal, which has been a revelation, and our listeners have just gone nuts over it.

One of the questions that came up was that some people were just being told that the key was unavailable. They had thought, well, maybe our mentioning it on Security Now! had slashdotted PayPal so there were no more keys to be had. But apparently it's only available in some regions?

MICHAEL: Yes. So let me give you a little background on what we're doing with Security Key. Security Key actually works on both your PayPal or eBay account. You can use it on both or either one of those two combinations. So it is truly a eBay, Inc. solution. Also we have just been in beta up until eBay Live, which was last month. So we've been pleasantly surprised by the amount of interest, the amount of customers out there like your audience that has come to us and said, please, I'm really interested in this. Please, I want one of these type of devices. Now, as any good kind of beta, we want to test the market, making sure that there is no bugs in the system, we have the right messaging or infrastructure. We only ran the beta in three countries, that being the U.S., Germany, and Australia, to make sure we had good geographic distribution throughout the world, different shipping issues, different language issues, et cetera, et cetera. And we went live in those three countries now.

So right now, regrettably, you have to live or have an account in one of those three countries in order to get one of the Security Keys. But next year we will be expanding the footprint to offer more countries. So I can't promise you exactly right now how many countries it'll be, but the goal is to whatever countries show strong interesting getting this, we will be working with our

individual units in those countries to expand this program to them.

Leo: I suspect you'll see a lot of interest from Canada.

Steve: I was just going to say, Leo...

MICHAEL: Yes.

Steve: ...our Canadian listeners will really be happy when we add them, so.

MICHAEL: Yes.

Leo: Can you describe, Michael, just for those who didn't hear us discuss it earlier, what we're talking about here, and how it works?

MICHAEL: Sure. Security Key is what they call OTP, or a one-time password type of device. It is a little piece of plastic that has an LCD display and a secure chip and processor inside of it that gives you a random code every 30 seconds. So if you think about it, think of it - the best analogy is to say it's like a PIN that you would add to your normal username and password. So a fraudster, a bad guy, needs to both steal this physical device from you, as well as steal your PIN, in order to be able to access your account. So it's the second factor is something you have, this little device, plus something you know, which is your normal password.

Leo: So a couple of things came up for me. I'm using one. I know Steve got one. And I love the idea because I have to say I have a lot of money - probably shouldn't say this publicly. But I have a lot of money in my PayPal account. That's where donations to TWiT go. And basically, because I get interest on my PayPal account, I use it as a bank account. Probably, again, not a good - well, all right, good, you don't mind that, then. But as a result I think the added security is great, and much better than a SiteKey or that stupid stuff that Bank of America is doing. I frankly trust you now more than I do BofA.

But a couple of things come up. What if I don't have my dongle with me? And in fact that happened to me last night. I wanted to pay for something, and you ask for secondary information. You say, you know...

MICHAEL: Yes.

Leo: ...the secrecy, the security question. Is that a kind of, I mean, in a way does that not undermine the power of the dongle?

MICHAEL: As you said before, you know, we've earned your trust over the years. We've shown that you can leave money in your PayPal account, and therefore you know it's trusted. No one's ever broken in and stolen, you know, into our network to actually steal all of our accounts. So Security Key, you think of it as an extra layer of security. It's an extra protection if you have that concern or if you do a lot of traveling and maybe need to access in a lot of public networks, or if you're having your computer go on the Internet to a lot of places that may get a lot of viruses, it's probably a good way to have that extra layer. But we don't want to make it so onerous that you can't use your account because you left your

key at home.

Leo: Which was - I was grateful because I leave my key at the office, and I was able to use it.

MICHAEL: Yeah. But right now we're just...

Leo: But in other words it's not really any different, though, than the way it's been before because, I mean, if I forgot my password I could go through many of these same steps.

MICHAEL: You could right now. As we get feedback, and as we get a better understanding of our customers' acceptance and usage, we may be, you know, updating and changing some of those flows where you don't have your key. But right now we're still, as I said, only in three countries right now. And that's kind of one of the reasons we're limiting our launch in three countries is to get feedback. Already our German audience has given us some feedback on this same process that we've made some tweaks based on their requests. So we're still kind of in that first step. We're only one month out of beta. And we are making adjustments based on feedback like yourself. So...

Steve: I thought I remembered that the process of purchasing without the key required a telephone call from PayPal to a phone number that was registered with our account.

MICHAEL: That is one way we can do it. There are different methods we can use, depending on what information you may have on file and what is your risk profile. So there's not a one-size-fits-all type of approach.

Leo: Ah, I see. So because I have a - I've been good, or my account hasn't had a problem, you were a little more flexible with me than you might have been with somebody else.

MICHAEL: Yeah. So we have a variety of mechanisms we can use if the customer says, oops, I forgot it at home. And that may be risk of transaction, risk of the profile. There's a lot of things behind the scenes we're doing to do that. And we'll keep on - we will keep changing that mix to improve it to make sure customers have a rewarding experience that is very secure, as well as doesn't hinder just the needs they have to have.

Leo: Well, it underscores the difficulty of doing something like this because you do face this convenience factor. And anybody who wants to improve security then faces pushback from customers who say, but it's inconvenient.

MICHAEL: True.

Steve: Yeah, the other, I mean, like, most often asked question we had was, hey, I really love this, but I have an E*TRADE account, and I use the same thing with them, and now I've got two. And am I going to end up with a keychain full of dongles that I have to drag around with me everywhere I go?

MICHAEL: I'm very familiar with the whole necklace problem, as we would call it, where you

have too many key chains. So one of the nice things about it, and one of the things that excited us most about Security Key, is we're one of the leading members of the VIP Network, which is - we're using VeriSign. VeriSign is a provider and provides infrastructure for Security Key. So other companies, other banks, other financial institutions may be involved. So right now you can use our token on those other institutions.

Leo: Oh, I like that.

MICHAEL: And so, you know, your same - so say whatever bank you want, whatever Web 2.0 company may be using it, any kind of institution you will be able to use this same token, and vice versa. So if you go to Bank X, and they issue a token, you can use that along as a VIP token on our system, and you can take ours on theirs. So we are eliminating the necklace problem because you should only have one token for all the VIP Network.

Leo: That's great. So it's kind of like a Plus Card network or so forth where people have all agreed to be participants.

MICHAEL: That is correct. So it is a very similar approach to establishing infrastructure so that everybody can confirm your identification and your strong authentication no matter whose dongle was issued to that.

Leo: Well, I have to say I wish BofA would do this instead of this stupid SiteKey, which I know is insecure, doesn't solve phishing issues because of man-in-the-middle attacks, and is a pain in the butt.

Steve: Well, and you know, Leo, the other thing that I remember is VeriSign is being aggressive with their support for OpenID.

Leo: Ooh, this could be an OpenID key at some point.

Steve: Exactly. I mean, that's what this means. If VeriSign would be an OpenID authenticator, then that means that it's not an expensive proposition for websites to begin to support this technology for authentication. I mean, using the same dongle that, you know, we got for $5 from PayPal. I mean, this is a major win.

MICHAEL: So, and I can't speak for VeriSign, I'm not their employee. But the goal is, you know, right now the VIP Network is a federated network, so you can use your identity and share that across multiple sites. As that grows, and as we prove to customers this is the value you should have, this is why you should adopt it, then you really get excited because you can open it up to new things like OpenID or CardSpace, something else, because all of those models fit very well with a federated infrastructure. So, again, the first step, I'm very excited by these new federated models; but we've kind of still got to prove the first step, customers want to use it, I prove to you, everybody else that this adds value. Then once I do that, all these new great doors open up.

Leo: I know our audience understands the value because we've done a whole two podcasts on multifactor authentication. What has been your experience with the public at large? Do they get this?

MICHAEL: We've been very surprised. Again, so I've been in security for a while. And I was coming in thinking that the interest, especially in the U.S., would be pretty small. However, we've been kind of almost blown away by the amount of customers that have been really interested and excited by adopting this and want to take part in their security, take a more active role. I think some of it is, like, really good form factor. I think some of it is regrettably so much phishing news has been out there, so much other education has been done that people realize this extra layer of security is needed because the Internet may not always be the safest place people think it is.

Steve: And I'll mention one thing, too, that happens as the single dongle becomes more useful, is then instead of it only being useful for PayPal, it's like, you know, the way we do things. Then, you know, Leo wouldn't be leaving it at home. It'd be worthwhile having it on your main key ring because you're going to make so much use of it.

Leo: Yeah.

MICHAEL: True. And we're also, besides that - and Leo may, even if we can prove the value, may still forget things because that may be a more fundamental flaw in his character.

Leo: How did you know?

MICHAEL: But we're looking at other form factors that you could do that would overcome this problem, too. And that's something else we're trying to do some testing on now and hope to have that next year also and to have more convenient form factors that leverage and may be embedded in some of the things you are going to carry with you, whether it's your phone...

Steve: [Indiscernible], yes, yes.

MICHAEL: You got it. So because, you know, everybody's life now, they don't live without their phone next to them or their iPod or something else. So there's different ways you can actually, instead of having to worry about something extra, embed it in something they know people will not forget. And that's also how we're trying to expand this program and reach a bigger audience next year, too.

Leo: Can you give me an example of how it might work on a cell phone?

MICHAEL: There's a couple of different ways. You could do something as simple as sending people an SMS message, so that instead of having your little dongle pop up with that number, you SMS somebody that number if they request it. And that's as simple as you get the SMS message and you type it in. And [indiscernible] that.

Leo: I'd like that. That would be very simple. It delays your transaction because you have to wait for the SMS, but usually that's pretty instantaneous.

Steve: Well, but also, Leo, there's nothing to prevent that crypto algorithm from running on the phone.

MICHAEL: That's number two. Thank you very much. Or you could download, or you could put an application on the phone or have something that could be embedded when you buy the phone that actually runs it on the phone itself. That's why there's kind of - there's a lot of different things on the phone you can do, and SMS is a very simple way to go. But there's a lot more elaborate, even more secure, with some of the cool things you can do if you actually place the application itself on the phone.

Leo: I'd love to see that. Boy, that'd be fantastic. But that also requires universal support. You know, again, you've got to get the cooperation of all the merchants and so forth.

MICHAEL: Well, I mean, in that case, if, you know, all the different people in the VIP Network or other kind of stuff, if your - that same - whether it's an application on your phone or an SMS message or any other kind of form factor, it would still work. So...

Steve: Right, because the idea is basically you guys are not doing it yourselves. You're using VeriSign's infrastructure and saying, you know, we want to authenticate this person, authenticate them using whatever message that that person has chosen.

MICHAEL: Yes.

Steve: And then it's all handled by that third party. And they come back and say yes, you know, this person authenticates.

MICHAEL: This is - you've summed it up very well.

Leo: Well, I cast a vote. I certainly think that's a great idea.

MICHAEL: Yeah.

Steve: We've got three votes here so far, Leo. And we've got 150,000 other listeners who are voting, too, so.

MICHAEL: No, and that's - we've also heard some of the similar feedback from our customers and beta customers about different form factors they want. And that's also what we're trying to do, especially if you look at other countries that may have a wider adoption of mobile, and maybe a safer, more accepted use of things like SMS in applications. How do I craft a form factor to meet their needs? And that's what we're trying to do.

Leo: Well, I'm excited. I think this is going to be a real boon to everybody. How widespread is the VIP Network? Is it the kind of thing that really kind of is going to be universal, or are there competitors, and...

MICHAEL: There are - there's a lot of companies that are involved. Off the top of my head right now I can't tell you all the key members that are public. I know a lot of different financial institutions here, especially in the U.S., have been interested in looking in it and are doing certain pilots. I don't know how many of those are actually public, so...

Steve: There's a lot of stuff going on that you can't talk about.

MICHAEL: I would say that for right now, to be cautious, I'd probably say that, yes.

Leo: Yeah, that's fair, that's fair. But it sounds like this is going to be kind of a big movement. I mean, and that's really going to be key, I think, to adoption of this.

Steve: And of course we're all hoping that there's not going to be another, you know, Blu-Ray versus HD or VHS versus Betamax.

Leo: Uh-oh, I think you dropped out there, Steve. We'll wait a second.

MICHAEL: We agree with that. We think that's the key.

Leo: Okay. Hold on just a sec. Hold on.

MICHAEL: Oh, can you hear me, or no?

Leo: I can hear you. Steve dropped out for a little bit. Restate your question, then, Steve.

Steve: So I guess what we're hoping is this is not going to evolve or devolve into a Blu-Ray versus HD or VHS versus Betamax sort of battle with other people trying to contend. I mean, from what we've seen so far, the idea, for example, that you guys are using VeriSign, VeriSign is a provider in this VIP Network. And we know that VeriSign is open to, if not already being an authenticator for OpenID, it looks like this is really achieving some critical mass.

MICHAEL: Yes. I totally, completely agree. And one of the things we're so excited by this is this is going to grow and be powerful via the same network effect that made PayPal and eBay so successful. It's people using it, people telling their friends, people saying, hey, I can use this same thing on multiple stuff. So we see that same network opportunity that we're experts and knowledgeable in taking place in the VIP Network.

Steve: Very nice. Well, it just - it really sounds like we've got, I mean, I'm glad you guys are doing this. It makes sense that something like PayPal would be the launch point because PayPal already is being used so extensively. And as you said, people have been made aware that the Internet's got dark places and boogeymen lurking around. And so there had - as you said, there's a tremendous need that you're answering. And then all of the sites where this would be nice to have but wouldn't have enough need for it to overcome inertia and to justify the cost of a dongle just for that, they get to come along for the ride and just enhance the overall value of the solution.

MICHAEL: Yeah. And that kind of - that's the reinforced network effect we're so excited about.

Leo: How many of your - you probably don't want to give out numbers of how many people have asked for this. Or do you?

MICHAEL: Right now I'd say we're exceeding expectations, but we're not in a position to give away hard numbers.

Leo: Right. Mostly PayPal people, or equal number of eBay people?

MICHAEL: There's been - equal.

Leo: Interesting.

MICHAEL: So there's been a lot of people on eBay because they want to make sure their eBay account, whether they're a seller or a buyer, you know, if you have a few employees or you're running a shop, you want to make sure that certain people get access to your account. So we've seen a good adoption across both businesses.

Steve: Is there any way to associate two dongles with a single account?

MICHAEL: Right now that isn't - right now you can only have one account per Security Key. We will be updating that later this year, the current plans are, so you can have multiple tokens that...

Steve: Beautiful. You know, because then you have one that you always leave at home, and you've got one that you take with you. And so you solve the problem of, like, leaving that one in the car or something. It's like, oh, I've got my home keys I can use. That's perfect.

Leo: Well, I don't really even want to carry it around. That's exactly how I'd like to do it is one at home and one at the office.

MICHAEL: Well, I call it my husband-and-wife problem. So my wife and I share a PayPal account. And, you know, we don't want to make sure she can't get access to our account. So having two tokens makes my marriage better.

Steve: And I'm sure I know the answer to this, but it was a question that we were asked. Somebody was a little freaked out by the fact that there was, like, a serial number on the back of the key. And they were concerned that that was giving away some sort of cryptographic information. And I was sure that what that meant was that that serial number referred to a database somewhere that was owned by the authenticating agency, like VeriSign. And so given that serial number, VeriSign has the ability to look up the actual crypto information to then apply it to the time of day and determine what the sequence should be coming from the token plus or minus 30 seconds, as opposed to that number on the back of the key being in any way directly usable by somebody.

Leo: Well, you use that number when you first activate the key.

Steve: Right.

MICHAEL: Yeah. So your explanation is basically correct. There is no personal information all about the number. All that number does is differentiate different tokens. Because each token has its own random piece of information put in it. So if I lined up all of our tokens together, they're not going to be producing the same number, you know, at the same minute because each of them has a different random number that then produces a unique number every 30 seconds. So...

Leo: But you need to associate that serial number with my account so you know what my number will be.

MICHAEL: You got it. That's it. So basically it's, well, you know, there's a 12345 token going to issue this number now, and what's the next number, what's the next number after that. And that's how those are correlated. So the serial number just makes sure that you can track and know what is the proper random number for...

Leo: If I lose my key, do you just send me a new one with a new serial number? You don't recreate that key.

MICHAEL: No. We would take that off. So if you lost it, we would eliminate that so no one else could use it. Plus we would give you a new one that would have a new random number inside of there that'd be producing different numbers.

Leo: I think this is a big step forward. I would love to see financial institutions do this. It eliminates the phishing problem.

Steve: Okay. And how can it be $5? I mean, that's what's so cool about this is it's five bucks. And, you know, and not 50.

MICHAEL: We're not - we're losing money. But that's - the goal here isn't to try to make money on this for security element. The goal here is how do we make sure our customers have something they can use to add an extra layer of security to their account. And in doing that, we believe that's in our long-term interests to do so.

Steve: I think that's just terrific.

MICHAEL: Yeah. And kind of...

Leo: You're not losing a lot. I doubt they cost that much to make. I mean, it's not like a hundred-dollar device.

MICHAEL: So also I've been asked a different question. People say, why don't you give them away? If it's extra security, you should give them to everybody. And what our studies and what our beta trial showed us was that, if you give something to somebody for free, they value it how much they paid for it. And that people that - a large number of folks that were given free didn't use it compared to people that paid $5.

Leo: So essentially the $5 is just earnest money saying, yeah, I really want this.

MICHAEL: Yeah.

Leo: Yeah. That makes sense, actually. Whenever I get free tickets, I never go to the concert. But if I paid for it, you better believe I'm there.

Steve: Well, no, and I think also it saves PayPal from, exactly as Michael was saying, of just having everyone click on, oh, yeah, I want one. And because it's so easy to click on a button if it's free. And then it comes, and it's like, oh, you know, I'll get around to it one...

Leo: So essentially you are giving it away. It's just this is a token amount to assure the interest of the customer.

MICHAEL: Yeah.

Leo: Yeah, I think that's fair.

Steve: And what do we know about the lifetime of the battery in this little thing, which is not changeable?

MICHAEL: They last, I believe, over three years, three to four, five years, something around that line.

Leo: I'll lose it before then, I know that.

MICHAEL: Yeah. And then if for some reason a customer, like it doesn't work, you contact us, we'll give you a new one. It's not as if, you know, if you say my token was working last time, and it's no longer working, you know, the numbers aren't coming up, we will - you can contact our support, and our support people will issue a new token.

Leo: I can't thank you enough for doing this. It just, you know, early on, you know, we use PayPal for donations to the TWiT network. And we've been very happy. We've been doing that for almost, well, over two years now. And occasionally we'll get, and it's not very often, but people have a long memory, and they remember the early days of PayPal where there were difficulties, frankly. PayPal was problematic. And I have to say I've been so happy with how that's worked for us. And it's little things like this that just kind of - I think they're important for PayPal to do. I think, Michael, hiring you, establishing this kind of office, and doing these little dongles really does make a difference in terms of reassuring people that this - and you have to because this is a new way of doing business that people don't understand yet. And they're not completely comfortable with it yet. But you've done a lot to raise my comfort level. I'm completely comfortable with it now.

Steve: PayPal has done something else that I stumbled on recently, and I just wonder if Michael has any involvement in this. PayPal now offers a virtual credit card service.

MICHAEL: Yes. I'm not directly involved in that, but I'm aware of the virtual debit card.

Leo: Is that a one-time number, or what is that?

Steve: Yes, Leo, it is a one-time number. It's a little app that you install, a little client that you install on your machine. It will...

Leo: I bet it's Windows only. Yeah, yeah.

Steve: Probably is at this point. Don't know.

MICHAEL: I can double-check on that one. I don't know off the top of my head.

Leo: What's the URL if I want to use that? Because I actually use a PayPal debit card. I'd prefer to use a one-time use number.

Steve: Oh, Leo, it is very cool. The way they've implemented it, it has both a form fill-in and the ability just to ask for a one-time use credit card number. And so it allows you, for non-PayPal sites, of course, to securely give them a number that's only good for that amount and that time, and then never again.

Leo: I'd be very - I would use PayPal all the time for that.

Steve: Well, I mean, it's working. I have it. I'm using it. It's fantastic.

Leo: So I have an existing debit card. Can I start using this other system instead, or...

MICHAEL: Yeah. Basically all that does is kind of obfuscate the card. So if you're using that on a site that doesn't take PayPal, the transaction would go through, but the merchant would never get access to your true...

Leo: I love it.

MICHAEL: So I don't have the URL right in front of me, so I could just email that to you later.

Leo: I'll find it. We'll put it in the show notes. The URL for the Security Key is very straightforward, it's PayPal.com/securitykey. $5, you have to be a PayPal or eBay member. I guess is it eBay.com/securitykey, as well?

MICHAEL: I believe so. You can link there from either the eBay or PayPal site.

Leo: So if you go to either one...

MICHAEL: Yeah. Then they'll redirect you to the order page. So you have to order it. And you can order it...

Leo: It does, in fact, eBay.com/securitykey does work.

MICHAEL: Yeah.

Leo: So I have an existing eBay account. I could probably now just link it up to my key; right?

MICHAEL: You just have to activate, that's all. If you already have the same key, you should activate it on your eBay account.

Leo: Excellent. Excellent.

Steve: Very cool.

Leo: Now if I could just get Bank of America to enter the 20th Century. I don't even care about the 21st. Just the 20th Century would be a nice start. Then everybody will be happy. Are they a VIP member, do you know?

MICHAEL: To my knowledge, no.

Leo: Yeah, of course not. Whatever bank is, that's where I'm going. If there's a bank that's doing this, I would go there now. I would change all my accounts, all the money that goes through Bank of America, I will go to this new bank, I don't care who you are, just use this key. That's all I ask.

Steve: I mean, especially with all of the pressure there is now to push people out of the offices and get them to do this stuff online. I mean, online banking, it needs to be made secure. I think, you know, if this acquires critical mass, it'll end up being, as you said, Leo, it'll be something people choose because that's - because they'll choose their lending institution based on the level of Internet security they provide.

Leo: And if they start using my cell phone, I'll move there. So there. Hey, Michael, thanks so much for your time. We really appreciate it.

MICHAEL: No problem. Glad I could help.

Leo: That was Michael Vergara, who is in charge of customer security at PayPal and doing a great job. I don't know, I feel like I was maybe over-effusive about the whole thing. But I just...

Steve: No, Leo, I don't think so. I think this - I think the fact that it's PayPal that is doing this, it's not some random, obscure website that's trying to get people to sign up. I mean, these guys have a strong adoption rate. Obviously we know, from all the excitement that our listeners demonstrated when I stumbled over this Security Key, that there's a strong interest there. And the idea that this is going to be a federated technology, I mean, I'm now, for a future podcast, I'm going to bring myself up to speed on what this whole VIP program is and find out what it

takes to - like how expensive it is, for example, to use it. The good news is, if VeriSign is, as I'm sure I read, I remember reading and mentioning even here on the podcast before, if they are friendly to OpenID, then they would be able to be an OpenID authenticator. And I'm hoping that means that all of this would be available for free...

Leo: Boy, that would be...

Steve: ...to a smaller website. You don't have to be a big - a PayPal or an eBay or some big mucky-muck. And then you'd be able to use the $5 dongle.

Leo: That's be super cool. Super cool.

Steve: And I want to also mention, because we did talk a little bit about the virtual debit card...

Leo: Yeah, while we were talking I tried to download it, and I can't. I don't know why, I'm on Windows, I click the button, it keeps sending me to some other page. So it's maybe not as straightforward as it ought to be. But it is an application Windows-only. I did find that out.

Steve: Okay, and it is in beta. It's another one of these things where we're jumping onto it at the beginning. I want to make sure that our listeners understand what this is. You know, you obviously caught it instantly, Leo, the idea being that - and as you said, other credit card services have made this available in the past. The idea is this gives you a one-time use, sort of virtual credit card number to use at any site, as Michael mentioned, that isn't supporting PayPal. You're able to ask PayPal for a one-time credit card number, which you give the site. The site then essentially uses, right then on the fly, PayPal to transfer the funds. But they never get your real credit card number, which is, you know, back tied to your PayPal account. So again, PayPal is insulating you so that you're not having to provide your sensitive financial information. It's just - it's tremendous.

Leo: And even if somebody steals it or gets it, it's only good once. So it's...

Steve: It's bogus from then on, right.

Leo: They can't do anything with it. Which is great. Yeah, I wish I could use it. By the way, apparently you don't need a PayPal credit card or debit card to use this. It acts as if you have one, but you don't need one. And I don't - I just tried it once on this XP system. Maybe there's something going on with it or whatever. But I'm going to keep trying because I'd love to get this set up and use it because, frankly, I use PayPal for everything. I really like it a lot.

Steve: Well, and again, for our listeners, if you put in "PayPal virtual debit card" into Google, up come a whole bunch of links.

Leo: That's how I found it.

Steve: And you can navigate around and find it.

Leo: Steve, we've wrapped up another thrilling, gripping edition of Security Now!. Next week we're going to do our mod 4 episode, I think.

Steve: Our mod 4. And we now know that the correct formula, as you mentioned, you reminded me again, is episode mod 4=0, so we can actually have Q&As. Otherwise we would have never been able to have another one.

Leo: You are a nerd. You are a nerd.

Steve: And it's going to be our episode, our big Episode 104, which is our two-year mark, so...

Leo: Excellent.

Steve: That's very cool.

Leo: I'm very pleased.

Steve: And then somebody's going to say, wait a minute, you really don't have two years. You're not into your - you haven't finished, you know, until 105. It's like, eh, okay, fine.

Leo: That's true. That's true.

Steve: Yeah, I know. I know, we have very attentive listeners, Leo.

Leo: All right, Steve. That wraps it up. We thank you so much for joining us, and we will see you next time on Security Now!.