SECURITY NOW!

Transcript of Episode #364

Mat Honan's Weekend

Description: After catching up with an eventful week of security news, Steve and Leo describe and explore the details of the "epic hack" that recently befell well-known technology writer Mat Honan.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-364.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-364-lq.mp3

SHOW TEASE: It's time for Security Now!. Steve Gibson's here, and it's very topical. We're kind of going to change up what we normally do. This would normally be a Q&A show. But given the big hack that happened to Mat Honan, writer for Wired magazine, Wired.com this week, Steve's going to talk about the hack, how it happened, and, most importantly, what lessons we have learned. Mat Honan's Very Bad Weekend, we'll talk about it next on Security Now!.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 364, recorded August 8th, 2012: Mat Honan's Very Bad Weekend.

It's time for Security Now!, the show that protects you, your loved ones, and your privacy, whenever you're online or off. Well, we can't protect you from some things, but we do our best.

Steve Gibson: And anywhere in between.

Leo: Anywhere in between. Our Explainer in Chief, Mr. Steve Gibson, is here, the man at GRC.com, creator of SpinRite, world's finest hard drive maintenance and recovery utility, lots of free utilities. We've been doing this show now, this is Episode 364. Which means normally, nominally, it would be a Q&A episode. Not so this time.

Steve: Well, yes. We had one set up for this week. Yet what happened was, late last week, on Friday, something happened to a well-known industry technology reporter, Mat Honan, involving - essentially he described it as the end of his digital life, I mean, a complete hacking of his digital life. You had him on your main TWiT podcast on Sunday, which I watched. And then he wrote about this in greater detail the following day, Monday of this week. And what we have, thanks to Mat's having untangled this and him having conversations with various involved parties, including the guys who hacked him, we believe, is now an understanding of how this was done. And I can't think of anything more on point for this podcast than us taking a close look at this.

And then, once we understand it, we'll discuss, Leo, how it happened sort of from a meta level; what our takeaways are; what, if anything, we can do; and sort of the state of the industry's security. So we'll catch up with news stuff. And then I want to share what Mat wrote on Monday and then take our listeners through sort of a forensic timeline that I've assembled from that because what Mat shares is a little bit out of sequence, and it's great for drama, but it leaves us a little not quite understanding how it happened. So I put it all together. And then we'll talk about what it means.

Leo: I would also be very interested in, yeah, in talking about what we do in response because it certainly made me completely rethink what I thought was a secure setup and change some things.

Steve: Yes.

Leo: And so I'd love to get your advice on that.

Steve: One of the things we're going to see - and again, we couldn't invent a more compelling scenario than what actually happened last Friday to this nice, well-meaning person. As a consequence, all the photos he ever took of his newborn daughter are hanging in the balance.

Leo: Well, there's good news I think on that. I think the forensics that Apple was able to do, the good news is that the overwrite hadn't happened yet. So I've hooked him up with friends of mine in the drive data recovery business up at DriveSavers, and I hope that he will get his pictures back. But that's the end of the story. We're going to go back in time to Friday in just a little bit. Also know you have some things to talk about including Mars. All right. Before we go to the "Honan Hack," as it is becoming known as, is there any other security news?

Steve: Well, the most interesting kerfuffle is - Ed Bott and a number of other people reported this. I mentioned Ed because he was also on TWiT on Sunday.

Leo: Yeah, love Ed.

Steve: Great old-timer in our industry whom you and I have known forever. And that is that Microsoft has announced that, indeed, IE 10, the next version of Internet Explorer, which will run on Windows 7 and presumably 8, will in fact have Do Not Track enabled by default.

Leo: Oh. So this - they went back and forth on this.

Steve: They have. Well, because there is such pressure against having this done coming from, as Ed described it, the "tracking industry." I got a kick out of that. I thought, oh, the tracking industry. There is a working group at the W3C that are putting together the specs for the Do Not Track header. And as we know, it's an optional request header, meaning that it's metadata, not part of the URL. It's additional stuff that the browser sends to the server for every request for pages and gifs and jpegs and images and scripts and everything. And so every request would be embellished with this little statement saying that this user wishes not to be tracked, wishes not to have this query tied into other queries, not to have cookies linked and all the tricks that are used.

And so we're aware now that many browsers, I think we're at all browsers at this point, can have this optionally, but normally it's disabled. Microsoft is the first, and I'm delighted because, as we know, I coined the term years ago "the tyranny of the default," which is sort of the expression I like to use for that most users don't go in and change things. They just assume that someone smarter than them chose the settings that are best for them, and so they just say "yes" a lot when they're asked questions.

So what that means is that, if it's enabled by default, it'll tend to stay on, which the tracking industry doesn't want to have happen. In fact, they're pushing the spec to state that browsers will have it disabled by default so then they can claim that Internet Explorer is not obeying the standards and can use that as their basis for ignoring the header. So we have a little ways to go. But it's clear that we're on the right track.

What Microsoft has said is that their express setup for IE 10 will enable it by default and make it clear that this is Do Not Track, that the request not to be tracked is enabled. And that'll be part of the express setup. If you use the custom setup, you'll be taken through more of a Q&A, like do you want this, do you want that, what do you want to be default search, do you want to disable - do you want to request not to have tracking? And even there I would imagine most people are going to say, yeah, I'd rather not be tracked. So this is a big event for the industry because Microsoft, even though most of us are no longer using IE, those of us within earshot of this podcast are probably on Chrome or Firefox with various...

Leo: It's still a huge number of people.

Steve: The majority, I mean, it's still got - it's still the majority platform.

Leo: Still the No. 1.

Steve: Yes. So what they do matters. And it does pave the way for other browsers that have added the header, but not yet taken the leap to enable it by default. It paves the way for them to do that. So that was this week's biggest news over on the security and privacy front. The other big news I got a kick out of, as I'm sure you did, in fact I guess Tom was up and broadcasting as Curiosity was making its phenomenal, multiphase, can-you-even-believe-they-pulled-it-off landing.

Leo: That's a good way to describe it. I had, and I think a lot of geeks did because I saw pictures on Instagram and stuff, many screens open. I had our live coverage. I had NASA. I had CNN, just to see what CNN was doing on the television. And CNN's shameful coverage was just ridiculously stupid. NASA was great. And we had some great interviews. We had Phil Plait, the Bad Astronomer. We had Steve Sell, the guy in charge of the crane. We had Dr. Kiki and, of course, Tom Merritt. So I was really proud of it. But you know what shocked me is how little attention this got. I'm shocked.

Steve: I'm with you completely. The next morning I specifically fired up a browser to look for news, and there was other stuff happening. I mean, it did collide with the Olympics, and that's been a major passion for people for the last week and a half. But still...

Leo: Yeah, well, that happens every four years. This has never happened.

Steve: Well, long-time listeners of this podcast will remember that I have always kept us aware of those cute little rovers, Spirit and Opportunity. Some dust storm would come up and cover their solar panels in red Martian dust, and then they would power themselves, they would wind down as their batteries discharged. And JPL, the Jet Propulsion Lab, would think, well, okay, that's probably it. They started in the beginning of '04, and these little suckers just kept going. I mean, they were the Energizer bunnies of Mars. And then a wind would come up a few months later, blow the red dust off of the solar panels, they would charge themselves back up and ping JPL. And it's like, oh, they're back.

Leo: [Happy machine noises]

Steve: And off they would go again. So who knows how long Curiosity is going to be driving around the surface. But with any luck we'll have many years of keeping tabs on it. So as I see things, I would love our people who are in Twitter to make sure that I know what's going on, and I'll pass that news on to our listeners.

Leo: It was so exciting.

Steve: It was fun to watch those two cute little guys who just kept on going, year after year after year.

Leo: Well, and, now, those were little guys. This is a science lab. I mean, this is a significant...

Steve: This is an SUV. We dropped an SUV on Mars.

Leo: Yeah, and it's got mass spectrometers, it's got the 3D stereoscopic camera, I mean, this thing, just the pictures we're already getting back are amazing. And I just can't wait to see what we discover. And it is a return, in some ways, I think, to space flight. The debate, of course, goes on and on about manned versus unmanned missions, and you can do so much with unmanned missions, and it's so much safer and less expensive. But I do think the reason there was less attention is because there was no human aboard. Had there been a human, of course, the world would have been mesmerized.

Steve: Yeah.

Leo: And that's why you put humans on these things. I don't know if it's a good enough reason. But that is why you do it.

Steve: Yeah, it's funny, I've watched our general sort of lack of interest. And people have, like, wondered, why isn't this generating the same sort of attention that our original space exploration was? And one of the things that has occurred to me is that, well, we don't have photon torpedoes. These are boring compared to the stuff that we now...

Leo: For chrissake, we hung a crane in the air and lowered the thing. It was about the coolest thing I've ever seen.

Steve: Oh, I agree. I mean, this really did happen.

Leo: This was almost photon torpedo quality, I'm telling you. But anyway, I do think that what I did see was that there was a bifurcation, that normal people didn't even know about it. But everybody who watches TWiT, I was in there with a community. There were a thousand people in the chatroom. We had more people watching that space coverage late at night than watched TWiT earlier in the evening. I'm convinced that the geeks, the Internet, the people who are into this stuff, were very much aware of it. And that's why we're going to do more of that kind of stuff here on TWiT. I think this is our job.

Steve: If Gene Roddenberry had written this landing sequence, and it was in one of the Star Trek episodes, we would have thought, oh, come on, you can't ever do that.

Leo: I thought, oh, come on. There's no way.

Steve: No, and this was real.

Leo: And they couldn't test it. It was too bizarre to even test. They just had to do it, and they did it. And brilliant.

Steve: Well, speaking of cars driving around Mars, we have cars driving around Nevada. Nevada granted Google a license for its driverless cars to drive on public streets. And the news came out that Google has passed 300,000 accident-free miles. And I saw something that I just didn't have time to drill down, but maybe you know more about this, where they said they were going to start allowing the cars to drive their employees to work.

Leo: I didn't see that, but that's great.

Steve: Before long. So...

Leo: Well, it's legal in California, or at least they've been doing it in California for some time. And I know that...

Steve: On public streets?

Leo: Oh, yeah.

Steve: Whoa.

Leo: Oh, yeah, for years. Now, I don't know if it is legal. I think that what they do is they - the guy's hovering his hands over the wheel or something. I don't know how they're getting away with it.

Steve: Very nervous copilots.

Leo: The state of California, along with the state of Nevada and several other states in the union, are passing these laws that will make this legal. I think this is very exciting. Notice, by the way, they said 300,000 accident-free miles, but they said 300,000 miles free of accidents while under autonomous control. The cars did have some fender benders while the guy was driving. It was the autonomous control that was safe.

Steve: Hal just says, "Dave, let go of the wheel, I've got this."

Leo: "I'm sorry, Dave. Take your hands off the wheel, Dave."

Steve: So on my stair climber I am reading "Kill Decision," which is Daniel Suarez's third book.

Leo: Awesome.

Steve: And I just wanted to recommend it.

Leo: It's good.

Steve: I'm reading it slowly because I only allow myself to read it when I'm huffing and puffing. But, oh.

Leo: He is so good, isn't he?

Steve: It is really developing nicely.

Leo: And tech topics, absolutely, I mean, he's so good on tech. And the topics that he covers are - you know he's going to be on Triangulation this afternoon at 3:00 p.m. Pacific, 6:00 p.m. Eastern time, 2200 UTC, Daniel Suarez. And I have so many questions for him. You know, is Raconteur real? Is there anything like this out there? It's just fascinating.

Steve: Yeah, he gets this stuff.

Leo: Oh, yeah.

Steve: Well, he gets the tech right so that it's satisfying. But it's very well put together.

Leo: There's some very challenging stuff in here. It's very interesting.

Steve: Yeah, it's great. Now, I heard you talking, I guess it must have been on Sunday when I had tuned in to listen to Mat and you talk, about "Total Recall," which I saw with Jen on Monday.

Leo: Oh, good. What did you think? Because I love the - it's a Philip K. Dick book, which of course is brilliant.

Steve: And I loved the old, the original Schwarzenegger movie.

Leo: "Get yourself to Mars. Why am I standing here with a towel on my head?" Great stuff.

Steve: There is a sense, and maybe it's me being as old as I am, where I'm feeling a little impatient with movies that just have action for its own sake.

Leo: I know, I'm the same way, and maybe it is age. There's just so much of it.

Steve: It's like, okay, come on, let's get on with the plot. It's like...

Leo: Another car chase? Really? Really?

Steve: Yeah, it's like those "Transformer" movies. It's just like, okay, we know we've got CG figured out. I can't tell the difference between what's real and not anymore, so thank you very much. But let's just not fill 45 minutes of the movie with gratuitous, nonstop action. That's just no longer that interesting. So I'm very excited about the new Bourne movie that comes out at the end of this week. And I'm glad I saw "Total Recall." But it's like, eh, okay.

Leo: I re-watched the old Arnold version, just getting ready for this. And it is a little dated, but it's such a fun movie.

Steve: It's just - it's well done.

Leo: I mean, kind of cheesy. It just has, you know, the '80s, well, they didn't have the computer effects and all that stuff. It all had to be real and rubber.

Steve: That had Johnny Cab in it, didn't it.

Leo: "You're in a Johnny Cab."

Steve: "You're in a Johnny Cab," that's right. I thought so.

Leo: Was there no Johnny Cab in the new one?

Steve: Oh, no, we didn't have that.

Leo: "You're in a Johnny Cab."

Steve: I mean, visually this thing was spectacular. And I said to Jen, as I remembered feeling when I was watching "Avatar," I'm wide-eyed, and I'm looking at these scapes, and I'm thinking, how do you make this movie? I mean, this is just - this isn't real, yet it looks perfect. I mean, just like huge city stuff that doesn't exist, and there it all is, fully imaged. Anyway, we're at a point now where we're just in sensory overload. It's just incredible what...

Leo: So you recommend seeing it, but don't expect a miracle.

Steve: Yeah, I think that "The Amazing Spider-Man" is still my favorite.

Leo: That's the one you liked the best, yeah.

Steve: And I saw, of course, the new Batman, or the final of the third. And it was good.

Leo: I liked it. I liked it better than I thought I would, to be honest.

Steve: Good, I'm glad you saw it.

Leo: It was better than I thought it would be. But I haven't seen...

Steve: And, boy, it's doing well in the box office.

Leo: Yeah, interesting.

Steve: I wanted to share a brief, actually almost only a couple of sentences, from a Mike Kruzel, who was kind enough - actually this was a posting in our newsgroup. I noticed that it's from grc.spinrite, which is the SpinRite newsgroup at news.grc.com. And he said, "I have two Dell Dimension 4600C computers, and the main computer I use crashed over the weekend, giving the message 'Primary hard disk 0 not found.'" That's never good. He says, "I ran SpinRite 6, and in about five hours it repaired the drive, and Windows booted back up. I did run Windows XP chkdsk in recovery mode, once before and then once after SpinRite. Thanks for its work. Mike."

Leo: Good.

Steve: So, yeah, another...

Leo: Usually, if you can't see drive 0, I mean, you can't see it, you can't fix it; right? I guess it was Windows that couldn't see it.

Steve: It was Windows that couldn't see it. But the BIOS, it was still physically there, so that was good enough.

Leo: Anyway, now, let's tell this story. Oh, boy.

Steve: Yes. So Mat Honan is a well-known technology writer. And this is a little dramatic, but this is the best way to introduce our listeners into what you and I now understand happened. And then we'll go back and build a timeline forensically because Mat puts this out in a little bit of a jumbled sequence.

Leo: And I have to say, first let me say right upfront, I've known Mat for years. Really like the guy. He's really the real deal, very smart. And, yes, he made mistakes, as we all have, I think, in time. But I'm grateful. I talked to him last night. He said, "This is a hard story for me to cover because it just kills me that this happened." But at the same time, and I told him this, he said, "I think I'm making a difference." I said "Mat."

Steve: Oh, he's done a service.

Leo: Huge service.

Steve: No doubt about it. So on Monday the story he wrote in Wired, in his "Gadget Lab" column, it was titled "How Apple and Amazon Security Flaws Led to My Epic Hacking." And as you said, Leo, as we'll shortly see, he's really not laying it all off on them. And our listeners will soon see that this can happen to anybody.

He says, "In the space of one hour, my entire digital life was destroyed. First my Google account was taken over, then deleted. Next my Twitter account was compromised and used as a platform to broadcast racist and homophobic messages. And worst of all, my Apple ID account was broken into, and my hackers used it to remotely erase all of the data on my iPhone, iPad, and MacBook.

"In many ways, this was all my fault. My accounts were daisy-chained together. Getting into Amazon let my hackers get into my Apple ID account, which helped them get into Gmail, which gave them access to Twitter. Had I used two-factor authentication for my Google account, it's possible that none of this would have happened because their ultimate goal was always to take over my Twitter account and wreak havoc. Lulz.

"Had I been regularly backing up the data on my MacBook, I wouldn't have had to worry about losing more than a year's worth of photos, covering the entire lifespan of my daughter, or documents and emails that I had stored in no other location. Those security lapses are my fault, and I deeply, deeply regret them.

"But what happened to me exposes vital security flaws in several customer service systems, most notably Apple's and Amazon's. Apple tech support gave the hackers access to my iCloud account. Amazon tech support gave them the ability to see a piece of information a partial credit card number that Apple used to release information. In short, the very four digits that Amazon considers unimportant enough to display in the clear on the web are precisely the same ones that Apple considers secure enough to perform identity verification. The disconnect exposes flaws in data management policies endemic to the entire technology industry and points to a looming nightmare as we enter the era of cloud computing and connected devices.

"This isn't just my problem. Since Friday, Aug. 3, when hackers broke into my accounts, I've heard from other users who were compromised in the same way, at least one of whom was targeted by the same group. Moreover, if your computers aren't already cloud-connected devices, they will be soon. Apple is working hard to get all of its customers to use iCloud. Google's entire operating system is cloud-based. And Windows 8, the most cloud-centric operating system yet, will hit desktops by the tens of millions in the coming year. My experience leads me to believe that cloud-based systems need fundamentally different security measures. Password-based security mechanisms which can be cracked, reset, and socially engineered no longer suffice in the era of cloud computing.

"I realized something was wrong at about 5:00 p.m. Friday afternoon. I was playing with my daughter when my iPhone suddenly powered down. I was expecting a call, so I went to plug it back in. It then rebooted to the setup screen. This was irritating, but I wasn't concerned. I assumed it was a software glitch. And my phone automatically backs up every night. I just assumed it would be a pain in the ass and nothing more. I entered my iCloud login to restore, and it wasn't accepted. Again, I was irritated, but not alarmed.

"I went to connect the iPhone to my computer and restore from that backup which I had just happened to do the other day. When I opened my laptop, an iCal message popped up telling me that my Gmail account information was wrong. Then the screen went gray and asked for a four-digit PIN. I didn't have a four-digit PIN [on my laptop].

"By now, I knew something was very, very wrong. For the first time it occurred to me that I was being hacked. Unsure of exactly what was happening, I unplugged my router and cable modem, turned off the Mac Mini we use as an entertainment center, grabbed my wife's phone, and called AppleCare, the company's tech support service, and spoke with a rep for the next hour and a half.

"It wasn't the first call they had had that day about my account. In fact, I later found out that a call had been placed just a little more than a half an hour before my own. But the Apple rep didn't bother to tell me about the first call concerning my account, despite the 90 minutes I spent on the phone with [him]. Nor would Apple tech support ever tell me about the first call voluntarily. It only shared this information after I asked about it. And I only knew about the first call because a hacker told me he had made the call himself.

"At 4:33 p.m., according to Apple's tech support records, someone called AppleCare claiming to be me. Apple says the caller reported that he couldn't get into his .Me email which, of course, was my .Me email. In response, Apple issued a temporary password. It did this despite the caller's inability to answer security questions I had set up. And it did this after the hacker supplied only two pieces of information that anyone with an Internet connection and a phone can discover.

"At 4:50 p.m., a password reset confirmation arrived in my inbox. I don't really use my .Me email, and rarely check it. But even if I did, I might not have noticed the message because the hackers immediately sent it to the trash. They then were able to follow the link in that email to permanently reset my [own] Apple ID password. At 4:52 p.m., a Gmail password recovery email arrived in my .Me mailbox."

Leo: Uh-oh.

Steve: "Two minutes later, another email arrived notifying me that my Google account password had changed. At 5:02 p.m. they reset my Twitter password. At 5:00 they used iCloud's 'Find My' tool to remotely wipe my iPhone. At 5:01 they remotely wiped my iPad. At 5:05 they remotely wiped my MacBook. Around this same time, they deleted my Google account. At 5:10, I placed the call to AppleCare. At 5:12 the attackers posted a message to my account on Twitter, taking credit for the hack.

"By wiping my MacBook and deleting my Google account, they now not only had the ability to control my account, but were able to prevent me from regaining access. And crazily, in ways that I don't and never will understand, those deletions were just collateral damage. My MacBook data including those irreplaceable pictures of my family, of my child's first year and relatives who have now passed from this life weren't the target. Nor were the eight years of messages in my Gmail account. The target was always Twitter. My MacBook data was torched simply to prevent me from getting back in. Lulz," he writes.

"I spent an hour and a half talking to AppleCare. One of the reasons it took me so long to get anything resolved with Apple during my initial phone call was because I couldn't answer the security questions it had on file for me. It turned out there's a good reason for that. Perhaps an hour or so into the call, the Apple representative on the line said, 'Mr. Herman, I....'

"'Wait. What did you call me?'

"'Mr. Herman?'

"'My name is Honan.'

"Apple had been looking at the wrong account all along. Because of that, I couldn't answer my security questions. And because of that, it asked me an alternate set of questions that it said would let tech support let me into my .Me account: a billing address and the last four digits of my credit card. Of course, when I gave them those, it was no use because tech support had misheard my last name.

"It turns out a billing address and the last four digits of a credit card number are the only two pieces of information anyone needs to get into your iCloud account. Once supplied, Apple will issue a temporary password, and that password grants access to iCloud. Apple tech support confirmed to me twice over the weekend that all you need to access someone's Apple ID is the associated email address, a credit card number, the billing address, and the last four digits of a credit card on file. I was very clear about this. During my second tech support call to AppleCare, the representative confirmed this [to me]: 'That's really all you have to have to verify something with us,' he said.

"We talked to Apple directly about its security policy, and company spokesperson Natalie Kerris told Wired, 'Apple takes customer privacy seriously and requires multiple forms of verification before resetting an Apple ID password. In this particular case, the customer's data was compromised by a person who had acquired personal information about the customer. In addition, we found that our own internal policies were not followed completely.'" I'll just interject here that that turns out not to be true. Continuing, she said, "We are reviewing all of our processes for resetting account passwords to ensure our customers' data is protected."

"On Monday" - so that's three days later, Monday the beginning of this week - "Wired tried to verify the hackers' access technique by performing it on a different account. We were successful. This means, ultimately, all you need in addition to someone's email address are those two easily acquired pieces of information: a billing address and the last four digits of a credit card on file. Here's the story of how the hackers got them.

"On the night of the hack, I tried to make sense of the ruin that was my digital life. My Google account was nuked, my Twitter account was suspended, my phone was in a useless state of restore, and for obvious reasons I was highly paranoid about using my .Me account for communication. I decided to set up a new Twitter account until my old one could be restored, just to let people know what was happening. I logged into Tumblr and posted an account of how I thought the takedown had occurred. At this point, I was assuming that my seven-digit alphanumeric Apple ID password had been hacked by brute force. In the comments" - and he says, in parens, "(and, oh, the comments)" - "others guessed that hackers had used some sort of keystroke logger. At the end of the post, I linked to my new Twitter account.

"And then, one of my hackers @ messaged me. He would later identify himself as Phobia. I followed him. He followed me back. We started a dialogue via Twitter direct messaging that later continued via email and AIM. Phobia was able to reveal enough detail about the hack and my compromised accounts that it became clear he was, at the very least, a party to how it went down. I agreed not to press charges, and in return he laid out exactly how the hack worked. But first, he wanted to clear something up: 'Didn't guess your password or use brute force. I have my own guide on how to secure emails.'

"I asked him why. Was I targeted specifically? Was this just to get to Gizmodo's Twitter account [that had been linked to mine]? No, Phobia said, they hadn't even been aware that my account was linked to Gizmodo's, that the Gizmodo linkage was just gravy. He said the hack was simply a grab for my three-character Twitter handle. That's all they wanted. They just wanted to take it, and [mess it] up, and watch it burn. It wasn't personal.

"'I honestly didn't have any heat towards you before this.'" I'm quoting. "'I just liked your username, like I said before,' he told me via Twitter direct message.

"After coming across my account" - which, by the way, is cool, it's "mat," so @mat, a very nice Twitter account, which he clearly, as you mentioned on Sunday, Leo, got very early.

Leo: Deeply regrets. And got it early.

Steve: He says, "After coming across my account, the hackers did some background research. My Twitter account linked to my personal website, where they found my Gmail address. Guessing that this was also the email address I used for Twitter, Phobia went to Google's account recovery page. He didn't even have to actually attempt a recovery. This was just a recon [mission]. Because I didn't have Google's two-factor authentication turned on, when Phobia entered my Gmail address, he could view the alternate email I had set up for account recovery. Google partially obscures that information, starring out many characters, but there were enough characters available, m****n@me.com. Jackpot.

"This was how the hack progressed. If I had some other account aside from an Apple email address, or had used two-factor authentication for Gmail, everything would have [been] stopped [there]. But using the .Me email account as a backup told the hacker I had an Apple ID account, which meant I was vulnerable to being hacked. 'You honestly can get into any email associated with Apple,' Phobia claimed in an email. And while it's work, that seems to be largely true. Since he already had the email, all he needed was my billing address and the last four digits of my credit card number to have Apple's [Care] tech support issue him the keys to my account.

"So how did he get this vital information? He began with the easy one. He got the billing address by doing a WHOIS search on my personal web domain. If someone doesn't have a domain, you can also look up his or her information on Spokeo, WhitePages, and PeopleSmart. Getting a credit card number is trickier, but it also relies on taking advantage of a company's backend systems. Phobia says that a partner" - that is, a partner of his - "performed this part of the hack, but described the technique to us, which we were able to verify via our own tech support [phone] calls. It's remarkably easy so easy that Wired was able to duplicate the exploit twice in minutes.

"First, you call Amazon and tell them you are the account holder and want to add a credit card number to the [existing] account. All you need is the name on the account, an associated email address, and the billing address. Amazon then allows you to input a new credit card." And he says, parens, "(Wired used a bogus credit card number from a website that generates fake card numbers that conform with the industry's published self-check algorithm.) Then you hang up.

"Next, you call back and tell Amazon that you've lost access to your account. Upon providing a name, billing address, and the new [credit] card number you gave the company on the prior call, Amazon [now allows] you to add a new email address to the account. From here, you go to the Amazon website and send a password reset to the new email account. This allows you to see all the credit cards on file for the account not the complete numbers, just the last four digits. But, as we know, Apple only needs those last four digits. We asked Amazon to comment on its security policy, but didn't have anything to share [at] press time.

"And it's also worth noting that one wouldn't have to call Amazon to pull this off. Your pizza [delivery] guy could do the same thing, for example. If you have an Apple ID, every time you call Pizza Hut, you've giving the 16 year old on the other end of the line all he needs to take over your entire digital life. And so, with my name, address, and the last four digits of my credit card number in hand, Phobia called AppleCare, and my digital life was laid waste.

"Yet still I was actually quite fortunate. They could have used my email accounts to gain access to my online banking or financial services. They could have used them to contact other people and socially engineer them, as well." Which actually is a point that Ed Bott brought up on your TWiT show the day before Mat wrote this. Oh, and he says, "as Ed Bott pointed out on TWiT.tv."

Leo: Oh.

Steve: "My years as a technology journalist have put some very influential people in my address book. They could have been victimized, too. Instead, the hackers just wanted to embarrass me, have some fun at my expense..."

Leo: Lulz.

Steve: "...and enrage my followers on Twitter by trolling. I had done some pretty stupid things, things you shouldn't do. I should have been regularly backing up my MacBook. Because I wasn't doing that, if all the photos from the first year and a half of my daughter's life are ultimately lost, I will have only myself to blame. I shouldn't have daisy-chained two such vital accounts my Google and my iCloud account together. I shouldn't have used the same email prefix across" - that is, his name portion - "mhonan@gmail.com, mhonan@me.com, and mhonan@wired.com. And I should have had a recovery address that's only used for recovery, without being tied to core services.

"But mostly I shouldn't have used Find My Mac. Find My iPhone has been a brilliant Apple service. If you lose your iPhone or have it stolen, the service lets you see where it is on a map. The New York Times' David Pogue recovered his lost iPhone just last week, thanks to the service. And so when Apple introduced Find My Mac in the update to its Lion operating system last year, I added that to my iCloud options, too. After all, as a reporter, often on the go, my laptop is my most important tool.

"But as a friend pointed out to me, while that service makes sense for phones, which are quite likely to be lost, it makes less sense for computers. You are almost certainly more likely to have your computer accessed remotely than physically. And even worse is the way Find My Mac is implemented. When you perform a remote hard drive wipe on Find my Mac, the system asks you to create a four-digit PIN so that the process can be reversed. But here's the thing: If someone else performs that wipe someone who gained access to your iCloud account through malicious means there's no way for you to enter that PIN.

"A better way to have this set up would be to require a second method of authentication when Find My Mac is initially set up. If this were the case, someone who was able to get into an iCloud account wouldn't be able to remotely wipe devices with malicious intent. It would also mean that you could potentially have a way to stop a remote wipe in progress. But that's not how it works. And Apple would not comment as to whether stronger authentication is being considered.

"As of Monday" - when he was writing this - "both of these exploits used by" - and I'm still reading from what he wrote. Mat writes: "As of Monday, both of these exploits used by the hackers were still functioning. Wired was able to duplicate them. Apple says its internal tech support processes weren't followed, and this is how my account was

compromised. However, this contradicts what AppleCare told me twice that weekend. If that is, in fact, the case, that I was the victim of Apple not following its own internal processes, then the problem is widespread.

"I asked Phobia why he did this to me. His answer wasn't satisfying. He says he likes to publicize security exploits so companies will fix them. He says it's the same reason he told me how it was done. He claims his partner in the attack was the person who wiped my MacBook. Phobia expressed remorse for this and says he would have stopped it had he known. 'Yeah, I really am a nice guy. IDK'" - I don't know - "'why I do some of the things I do,' he told me via AIM. 'IDK, my goal is to get it out there to other people so eventually everyone can overcome hackers.'

"I asked specifically about the photos of my little girl, which are, to me, the greatest tragedy in all this. Unless I can recover those photos via data recovery services, they are gone forever. On AIM, I asked him if he was sorry for doing that. Phobia replied, 'Even though I wasn't the one that did it, I feel sorry about that. That's a lot of memories. I'm only 19, but if my parents lost the footage of me and pics, I would be beyond sad, and I'm sure they would be, too.'

"But let's say he did know and failed to stop it. Hell, for the sake of argument, let's say he did it. Let's say he pulled the trigger. The weird thing is, I'm not even especially angry at Phobia or his partner in the attack. I'm mostly mad at myself. I'm mad as hell for not backing up my data. I'm sad and shocked and feel that I am ultimately to blame for that loss.

"But I'm also upset that this ecosystem that I've placed so much of my trust in has let me down so thoroughly. I'm angry that Amazon makes it so remarkably easy to allow someone into your account, which has obvious financial consequences. And then there's

Apple. I bought into the Apple account system originally to buy songs at 99 cents a pop, and over the years that same ID has evolved into a single point of entry that controls my phones, tablets, computers and data-driven life. With this Apple ID, someone can make thousands of dollars of purchases in an instant, or do damage at a cost that you can't put a price on."

Leo: Well, and I'll give you a couple of PS's.

Steve: Yes.

Leo: First of all, the good news is - you know, I don't know why Apple didn't ask Phobia for the PIN. Maybe he did, and it wasn't given to him. But Apple was able to apparently brute-force it because it's only four digits. And they say that the data will be on that hard drive. So I've hooked the man up with the folks at DriveSavers, and I think they'll be able to get his data back.

Steve: Good.

Leo: So dodged a bullet on that one. The other good news, and I'm sure you're going to say this, but we should say it right upfront, is that both Apple and Amazon have, in response to this, changed their systems.

Steve: Yes.

Leo: Amazon permanently; Apple, it's not clear.

Steve: Yes, exactly. So, okay. Let me just - I'm going to briefly recount in sequence, adding a little more detail than Mat did. So this began sometime mid to early afternoon on Friday, August 3rd, when one or more hackers just took a shine to an unknown person's Twitter account because they say it was three characters. It was @mat. They didn't know anything about him. Didn't know who he was, just thought, hey, that's cool. And I don't know how many followers he had. I checked yesterday, and it was not hundreds of thousands. So maybe they got lost in the account transfer or freeze or something. I mean, it didn't look like there was a huge - it's nothing like what you have following you, Leo. So I don't know. Or maybe it's because it's linked to Gizmodo.

Leo: It's so complicated. He may not have been able to bring his followers with him. And by the way, these guys, and I have corresponded a little bit with Phobia on Twitter, and his partner in crime, and they've got something going on because his partner in crime has a Twitter account that has 122 tweets and over 100,000 followers. So there's something going on. My suspicion would be they have more access to Twitter than they have acknowledged. There's something. Or maybe they've created 100,000 bots. I don't know.

Steve: Well, so apparently, not knowing anything about Mat, but just liking @mat, they do some recon. They see that, from the information on his Twitter account, @mat, which is where this whole thing starts, that account links to honan.net, which is Mat's personal website. They go there, and they find his Gmail account, mhonan@gmail.com. They access Gmail's account recovery, putting that in as their email address. And because there's no additional protection - and this is what we're going to talk about here in a second, Leo. The lack of two-factor authentication means that account recovery information is unprotected, and that account's alternate email address is visible, but obscured. So what they see is m****n@me.com.

Leo: Don't really have to guess what those are.

Steve: No. They already saw mhonan@gmail.com. So they realize, okay, he's used - and that's what Mat refers to in the article as using the same first name across his accounts. So that of course allows them to guess Mat's Apple ID and Cloud address. The hacker also does a WHOIS search on Mat's personal web domain to get more information. Now, I've done that, and you could do that, Leo. I'm not going to share what it shows because it's horrifying.

Leo: Yeah. This is an argument for WHOIS privacy.

Steve: I'm annoyed that, at least if you're a Network Solutions customer, as I am, they want to charge you to obscure this.

Leo: I should point out that Hover does not. So if you do a WHOIS on our TWiT.tv or any of our sites, you'll get the administrative contact and technical contact addresses will be a company called Contact Privacy in Toronto, Canada, not us.

Steve: And that does not cost you anything?

Leo: No. That's one of the reasons I like Hover.

Steve: Good. So what's here in this WHOIS is, right now, I mean, I did it an hour ago, and it's like, okay, Mat, fix this because here is way too much information exposed publicly still. So Wednesday morning. Okay. So now they've got his street address. They've got his, I don't know if this is a landline or a cell phone, but that's there, too. And ZIP code, the works. And a bunch of email addresses. So now someone calls Amazon wanting to add an additional credit card to Mat's account.

Leo: Now, this is kind of, I think, key because this is social engineering, not a technical hack. This is not a MySQL attack.

Steve: How many times are we arguing about how many bits the crypto key has to have?

Leo: Right, right.

Steve: No bits came into play here.

Leo: Right. I don't consider doing a WHOIS anything particularly technical. And that's really all they were doing. This is social engineering, 100 percent.

Steve: Well, and also, frankly, I am really glad that this whole story came to light and that Mat, I mean, I'm so sorry for his loss of data and the embarrassment and everything. But the way Amazon was set up, and as you said, they are no longer, and that's like, thank goodness. But someone was very clever to put this together. Here's the Amazon portion.

So you call Amazon on the phone, and you say you want to add an additional credit card. What do you need? The name, which of course they have, Mat Honan; the email address associated with the account. Now, they guessed that he would be using Gmail. He was, so mhonan@gmail.com. There were two ways to get that: Twitter to website to Gmail, or WHOIS because Mat's WHOIS had that, too. And as we know, email addresses are not hard to find. And the billing address, which they got, right there, from WHOIS. So that allowed them to invent a credit card and stick it on the account.

Then they hang up, and they call back. They're going to get somebody else. Now they say they've lost access. What do you need to gain access? The name, which we already know they have; the billing address, which they have; and the last four digits of any one credit card registered on the account. So they gave the four digits of the one they'd just added a second before, and that allowed them to add a new email address to the account. So now they've added an email address they control, which they don't yet have.

Then they go to the website and say, we can't log in. Send us a password reset. So, and we're going to see this a bunch, and this is one of the issues that this whole thing brings up is the use of email for password recovery, which is the weak link in much of this. So they get an email address they control into the account, ask for password reset. That sends them a link allowing them then to log into Mat's Amazon account, where they can see everything he's ever purchased and all of his actual credit cards. Well, they see the one that they just spoofed and added, and they see his real one.

Now they have the last four digits of Mat's main card, and they've already got his name, email addresses, and billing address, which is the same as his home address. So at 4:00 p.m., with all this information, the hacker calls AppleCare, impersonates Mat, claiming that he'd forgotten the password to his mhonan@me.com account, which they now know.

Leo: These guys, I'll say one thing, they're ballsy.

Steve: They are, yes.

Leo: They've got a lot of nerve. And I think to do this you have to be good at acting.

Steve: Yes.

Leo: I think.

Steve: Yes, I completely agree. You've got to sound convincing. Although, frankly, I've had some calls from my credit card company where I wished the other guy was an actor. I can barely understand what he's saying.

Leo: Yeah. Maybe not. Apple can't make a judgment about its users. And this is the whole point is Apple is trying to make it easy for users.

Steve: Yes. Unfortunately, these systems fail open, rather than failing closed. So he says, "I've forgotten the password, mhonan@me.com. I need a temporary password so I can access my account." Despite the fact that the hacker fails all the security questions, doesn't know any of Mat's security questions, the backup that Apple provides, or provided, maybe that's over, we're not sure yet, is, well, if you can't remember your security questions, how about your billing address and the last four digits of your credit card that they have on file? Which of course they now have, thanks to the game they played over at Amazon.

Leo: Probably other ways to get it, too. It's fairly easy to do this; right? I mean, it's not much to ask.

Steve: Well, and this was also the point that he makes about the Pizza Hut guy.

Leo: He knows that.

Steve: When you phone for pizza, you give them your address because you'd like it delivered, and you give them your credit card number over the phone. So they've got that. And how many places now are we seeing people asking for your email address because we'd just like to inform you of any...

Leo: Stay in touch, yeah.

Steve: Yeah, exactly. So Apple issues a temporary password which allows the hacker to log into iCloud and Mat's mhonan@me.com email account. And this is - this is one point that's important - this is in keeping with Apple's official Care policies at the time. This was not a mistake. And that's a point that Mat made, and I've read similar things coming at this from different directions about this earlier this week. So it is not the case that that one spokesperson misspoke.

Okay. That was at 4:33. At 4:50, Apple sends the password reset link to Mat's mhonan@me.com account. The hackers log in with a temporary password. They receive and delete the password reset email, not that it really matters, and they reset Mat's password, locking Mat out of his own Apple ID and iCloud account. Two minutes later, 4:52, Google Mail password recovery email arrives at Mat's mhonan@me.com account.

So what they did was they went back over to Google, where they had visited before, where they saw that he had a .Me account. They do password recovery at Google which sends the recovery link to the .Me account, so they click that. That gives them access to Mat's Gmail account. They change his Gmail password, locking him out of his Gmail account. Two minutes later, 4:54, mail arrives at .Me informing Mat, who can no longer log into there, either, that his Google Mail password has been changed. So the notice goes out that the password change has been effective, but Mat can't see that because he's already been locked out of his accounts.

A few minutes later, at 5:00 p.m., with access to Mat's Apple ID and iCloud account, hackers remotely wipe Mat's iPhone. A minute later, at 5:01, they remotely wipe Mat's iPad. A minute later, at 5:02, the Twitter account password is reset, so a reset comes. The password is changed. So they now have taken over his Twitter account, Mat's locked out of his very cool @mat account, and hackers have achieved their intended goal. A couple minutes later, having verified that, at 5:05, to prevent Mat from having any tools to regain control, they remotely wipe Mat's not-backed-up MacBook containing, as we know, his only copies of his newborn daughter's photo collection and pics of older relatives who've passed away.

At 5:10, five minutes after that, Mat notices his iPhone has been cleared and places his first 90-minute call to AppleCare. Two minutes later, hackers, having control of @mat Twitter account, post a message to Mat's account taking credit for their actions. So Wired successfully repeated many of these alleged hacks, verifying them through the weekend and into the beginning of the week. Apple has reacted, as reported by Wired. Wired said:

"Apple on Tuesday" - so that's the day before we're recording this, that would be Tuesday the 7th. "Apple on Tuesday ordered its support staff to immediately stop processing Apple ID password changes requested over the phone. An Apple worker with knowledge of the situation, speaking on condition of anonymity, told Wired that the over-the-phone password freeze" - on obeying this change request - "would last at least 24 hours. The employee speculated that the freeze was put in place to give Apple more time to determine what security policies needed to be changed, if any."

When Wired tried the exploit again: "The representative said that the company was going through system-wide 'maintenance updates' that prevented anyone from resetting any passwords over the phone. The rep said we should try calling back after about 24 hours, and directed us to iforgot.apple.com to change Apple ID passwords ourselves [using] the web instead. 'Right now, our system does not allow us to reset passwords,' the Apple rep told Wired. 'I don't know why.'

"In an earlier attempt on Tuesday to change an Apple ID password (which is the same password used to log into iCloud and iTunes), Apple customer service offered up a different response, saying that passwords could only be changed over the phone if we were able to supply a serial number for a device linked to the Apple ID in question for example, an iPhone, iPad or MacBook computer. The rep also suggested changing our Apple ID password online at appleid.apple.com or iforgot.apple.com."

On the Amazon side, also via Wired: "Amazon changed its customer privacy policies on Monday, closing security gaps that were exploited in the identity hacking of Wired reporter Mat Honan on Friday. Previously, Amazon allowed people to call in and change the email address associated with an Amazon account or add a credit card number to an Amazon account, as long as the caller could identify him or herself by name, email address, and mailing address three bits of personal information that are easily found online.

"On Tuesday, Amazon handed down to its customer service department a policy change that no longer allows people to call in and change account settings, such as credit cards or email addresses associated with its user accounts. Amazon officials weren't available for comment on the security changes, but during phone calls to Amazon customer service on Tuesday, representatives told us that the changes were sent out [that] morning and put in place for 'your security.'"

Leo: Good.

Steve: So there is the story. Yes. Very, very good.

Leo: So what have we learned? In other words, I think the think that people really want is to know, well, what should I be doing so that I can make this harder? I don't know if you could make it impossible, but what should I be doing to make it harder?

Steve: Clearly, the thing - how many times have we seen that convenience is the enemy of security? What was so convenient for Mat was, first of all, that mhonan was the same email, whether it had the suffix of Gmail or .Me or - there was another one. There were three.

Leo: You don't want readily guessable email addresses. So that's No. 1.

Steve: You don't want that.

Leo: You could guess my email address on every service I use. Every one.

Steve: We all know your email address, Leo.

Leo: Yeah. But, I mean, so I failed at that. And it would be a bit of a pain to go change all that, to be honest. I have to get new accounts.

Steve: In fact, we made the comment last week when we were talking about Outlook.com, that there was a land rush to log in and lock down...

Leo: Right, get your name.

Steve: ...your name on Outlook.com.

Leo: But truthfully, knowing my email address, because I'm never going to have a -

knowing my email address shouldn't - I guess what I could do is create some dummy email addresses that are the ones I use just for accounts and account verification; right?

Steve: Well, yes. That's the big problem. So on one side, one aspect of convenience was that Mat happened to use mhonan as an available account name across his services, such that it was obvious for the attackers to make the jump from his Gmail email address over to his Apple ID address, just by guessing. So there's that. But the main focus of convenience is that Gmail - everything pointed to Gmail. His Twitter account recovery was Gmail. His Apple ID recovery. His Amazon billing address was Gmail. Everything went there, which was also where he conducted all of his other business. His website pointed there.

So that single account makes a person's life very much easier. But unfortunately, that's the source, that's the major aspect of insecurity over which we have control. We have no control over Amazon's policy. And frankly, this was tricky enough that this gives me the creeps because I know from the dialogue that you shared with me that you had with these people we believe them to be, I guess last night, they said they know how to do this kind of thing against other services.

Leo: Right. I asked him, I said, if you were going to hack me, how would you start? And he described this process. He says, well, the first thing we want to do is get as much information as publicly online. We search for you. We want your "docs," he called them.

Steve: Right.

Leo: And the problem is a lot of this stuff is online. Even down to home address, which is, if you've ever bought a house, is public information. It is out there. Or contributed to a campaign, or any number of things.

Steve: We're also seeing a trend, I mean, I'm seeing this in the news, that the next generation of people growing up in this social networking environment, they sort of take it for granted, and they're putting their lives online. There are people who are regretting it now because I'm seeing, for example, that in employment interviews they're asking for all of your social networking account names so they can go do research on you. They're not using a rsum, they're going out and looking at your Facebook and who are your followers and digging into your lives. So the people who are growing up in this environment, to a greater degree than you and I, Leo, I mean, I just checked, do I have iCloud on anything, or the "wipe my device," and it's like, no. I just sort of...

Leo: That is a very risky thing. And yet handy, especially for a laptop. I mean, to be able to wipe your portable device is great if it gets stolen. It's a form of security. The problem really is that Apple makes it a little too easy for somebody to hijack your account and then wipe your stuff.

Steve: Well, yes. And that's a problem that is an outgrowth of the real problem, which is to this day the only means, the universal means for authenticating someone is demonstrating control of an email account. That's the issue. Are you the person who receives mail? Now, the really frightening thing, I mean, if we want to look at that, is that email is unencrypted. This is all going across the wire in plaintext. Web sessions increasingly, as we know, are protected by SSL, HTTPS. But email generally is not. And so here are all these links for account recovery flying back and forth, and those are literally the keys to the kingdom.

So the problem is that, even today, in this day and age, at this point we don't - nobody has YubiKeys built in. We're not all carrying Google Authenticator or VeriSign Identity Protection tokens or the "something you have" approach. Which is why I loved that little tidbit we just heard about Apple sort of experimenting with you need to tell us the serial number of your device.

Leo: That's a good one, yeah.

Steve: Yes. That's good. That's not something...

Leo: Of course, if your device has been stolen...

Steve: Yes. And unfortunately, once it becomes widespread, it'll be like your Social Security number. It'll be posted and available and in databases for people to check and so forth. So unfortunately we're just really bad at managing this kind of information. I'm annoyed, for example, when I get statements like privacy statements from my credit card companies, and they're saying unless you send this back and tell us no, we're going to do the following things. And I look at what they're - and it's like, share your personal information with our business partners. Unspecified, just anybody who we think we want to do business with, unless you tell us we can't. I say, wait a minute? Why is this opt-out rather than opt-in? So that's a problem.

But back to what we can do. We know there are beginning to be second-factor authentication. One of the problems is, these hackers whom you had the conversation with and whom Mat spoke with, they said, all we need is information. Information. When, you know, they made phone calls. The essence of these attacks, as you said, they had to be rather bold because this was not something done all online. This was people on the phone providing information. So there was nowhere here, as we have discussed in multifactor authentication many times, something you have. This was all something you know. It was security questions, it was last four digits of your credit card number, all of this something you know, not something that you physically possess.

So I would say that the right thing to do, the best thing we could do - because, again, we cannot control the policies of all the companies we do business with. I'm glad this happened. I'm glad Amazon got a wakeup call. I'm glad Apple got a wakeup call. They're two biggies, but they're not certainly the only people that may have hackable policies.

Leo: Well, and these guys claim they have many other companies with similar bad policies that they can take advantage of.

Steve: Precisely. So you really want to bifurcate your - because email confirmation loops are the only way we have, still, for doing password recovery, you want to consciously separate completely an email account for those sorts of purposes from the ones you normally use during the day. It's going to be less convenient. It would be much easier if they were all going to the same place. But you'll want to use a different account name. You'll want to use a domain name, maybe, that is different. But you also want an account where, to the best of your ability, it looks like they honor tight recovery.

I know, for example, even PayPal, I'm set up with my football that I'm still using, the six-digit time-varying code, and a VIP token on my phone, so I'm able to use it when I'm away from home. But right there, underneath the challenge for those, is "Click here if you don't have it with you." What?

Leo: Right. Almost every time. Right. Because, again, convenience trumps security.

Steve: Yeah. The point is, I'm promising I'm going to have it with me. And I went looking around. Is there any way I can say take that exception off? I want the security of having to have what I'm telling you I will have, and you're telling me I have to have, except you're telling me I don't have to have it.

Leo: Right, yeah. So you've got to wonder, well.

Steve: Yeah.

Leo: And that's the problem, by the way, with security questions because people don't remember them. Then they go, okay, well, you don't need it. All you need is the last four digits - or they did. All we need is...

Steve: We're sorry you forgot your question.

Leo: Just give us your email and last four, we'll call it a day.

Steve: Yeah.

Leo: You know, I wanted to ask you specifically about two-factor authentication on Google.

Steve: Yes.

Leo: And Google has a particular problem. Now, Facebook has turned on, or has available and you should turn it on, two-factor authentication. And what it will do is it will send a code - actually, you have to use the Facebook app on your smartphone. It will give you a code which you can then enter if you're going to log in on an unrecognized machine. I think that's great. The problem with Google...

Steve: So that probably means that they leave a persistent cookie on the machine.

Leo: They do.

Steve: And then from then on...

Leo: It's a known machine; right.

Steve: ...when that machine is being used. Okay, that's cool.

Leo: And you can, I presume, you can revoke those cookies and so forth. I'm pretty sure there's somewhere you could say, I don't recognize any of these devices, let's start over.

Steve: Right.

Leo: Now, Google has second-factor authentication, but it's more tricky for Google because, not only do you log into your Google account on the web and on Google applications, both of which understand second-factor authentication, there are a great many third-party applications that do not. So what Google is required to do, if you turn on second-factor authentication, is give you one-time-use passwords which are all, by the way, alphanumeric. Now, they're only one-time use, so that's probably okay. They're not strong passwords. And now, for instance, if I want to use - I have a calendar app that I use that uses Google Calendar. Instead of using my Google password to log into this, I have to use this one-time authentication code. And then, it's a pain in the butt, but that expires, in some cases every 30 days, in some cases in unknown ways. And you've got to go generate another one and use it again.

And that seems to me, besides being a pain in the neck, and I keep trying to turn this thing on, and I always turn it off because I have so - I'm a little different than most people. I have many, many devices with many - and they're all logging into Google eMail, Google Calendar, Google Voice. That means I have to enter these in all the time. I have dozens of one-time passwords. It seems to me, if I have a strong password on Google and - and this I think is the most important thing people can do on Google - have attached a cell phone number for account recovery to it, that's not done by default...

Steve: And not link it to another address...

Leo: And link it to a separate address that nobody knows, which I've done, that that's going to be as good as the second, well, not theoretically as good, but practically as good as second-factor authentication, and certainly...

Steve: Yes. And more practical for you to use because, as we know, if it becomes a pain, it'll get turned off.

Leo: Right.

Steve: Despite our best intentions and our desire to be secure, convenience will trump that, ultimately.

Leo: Right. If everything supported second-factor authentication, I could use that Google Authenticator to generate that, then I'd be happy. I don't mind entering my password and a code for my cell phone. But having to go back to the web, get a one-time-use password, enter it in, and it has to be entered manually in many cases because I can't cut and paste because it's not on the same device...

Steve: Now, are these, like, startup problems where the two-factor authentication has not yet permeated Google's ecosystem?

Leo: I would guess, yeah. It's not Google. These are third-party apps. So a lot of apps, for instance, are designed to get Gmail. But they're not Google apps.

Steve: Oh, I got it.

Leo: Or to get your calendar. But they're not Google apps. So even desktop apps. So you can no longer, because you've turned on second-factor authentication, just use your Google password to open those apps up. So Google creates for you a one-time-use password.

Steve: And do you want to use those, or do you have to use those?

Leo: You have to use those.

Steve: Okay. No, I meant those apps.

Leo: Oh, well, if I'm using a smartphone, yeah. So if you're using an iPhone, for instance, it doesn't support the second-factor authentication. You have to use this one-time pass to get in there. And that one-time pass, again, I think it's 12 digits, or 12 letters. It's alphanumeric, all uppercase. So it's not super-secure one-time use, I gather, but I'm not convinced. And I have seen that there are ways to bypass. So I've decided that it's just too inconvenient. I'm not recommend this to people. You should all turn on second-factor authentication on Google. But for me it's just too much trouble.

And so in fact what I'm doing is I've got an account recovery phone number. I think that that's a good way. If he had had that, he could have recovered his Gmail account, changed the password, and they would have been locked out again. Now, in the interim they would have gotten in to everything else, but...

Steve: Yeah. Actually it was their access to Gmail that allowed them to get to Twitter. And that was really where they wanted to get. So it was because Twitter was pointing to Gmail, as was Apple, as was Amazon, everything was converging there on Google Mail because Mat is Google-centric, as a huge number of us are.

Leo: Most of us are. Many of us are, yeah.

Steve: Yeah.

Leo: So diversity, heterogeneity is a very good idea.

Steve: Yeah. And being conscious of the fact that, unfortunately, where we are today, email password recovery is the only universally available solution, so it's what everybody offers. And unfortunately, it's not something you can turn off. It would be nice if there was a way to say I will take responsibility for this. The perfect example is I've talked about how I can't buy gas with a particular credit card because they just shut it down when they see it at a gas pump. And I've said, can I please override this? And they go, no, sorry, you can't. So there are no options typically for disabling account recovery. Maybe, well, no, you can't not have an email address.

Leo: I truly - what I actually believe is that we're all vulnerable to some degree, and that you should do the best you can. But we're somewhat at the mercy of these third parties.

Steve: What was creepy - and I've talked about how porous security is, that it's more porous than we think - what's creepy is that it was a whim. These one or more people just decided, ooh, look, @mat, that would be - it'd be fun to post to that Twitter account. Let's go do that. And they were able to. There was huge collateral damage, as Mat described it, as a consequence of their simply wanting to send tweets out through his Twitter account. So you've got to wonder how safe we are to somebody wanting to get us.

Leo: I'm not clear, by the way, these single-time passwords, I have to ask Matt Cutts. There's unclarity in my mind about how - they do not expire, but I am told that, once you use one, you can't reuse it.

Steve: That would make sense. Thus "one-time."

Leo: I would think that's how it is. They're called "application-specific passwords." And you can revoke them at any time. But you have to go to the website, log into

Google using two-factor authentication, and revoke them.

Steve: It would be nice if - again, lots of things would be nice. What Facebook is doing does raise the bar, the fact that they provide a secure cookie. I'm sure it's flagged secure, meaning that it will not be divulged over a non-SSL connection. So you have HTTPS secure connection to Facebook, which we know they have. We've seen these changes, and we've discussed them as they've been occurring over the last couple years. So there's a cookie that only that machine has that will only send in a query over a secure connection from your browser, which identifies it to Facebook as one that has been seen before. So that's a nice barrier. So that is allowing Facebook to painlessly tag devices that you have in the past logged in from and allow you to do so again. That would be some nice tech for Google to add. One wonders why they don't yet.

Leo: Yeah, I mean, I think we're in a world where we have to balance convenience with security. And so inevitably there are going to be flaws.

Steve: Yes. I guess the main takeaway, the only real takeaway I can suggest from this fun, I mean, sad but really gripping adventure with Mat, is consider separating accounts that could be used for password recovery so that - and really, it's not clear that you want a single account. You kind of want a family of accounts. And that really becomes a pain, if your main services all need to point somewhere different. Boy. The problem is using email for this is just really - that's the source of major insecurity. And I don't see that going away anytime soon because there's nothing to replace it until we get good "something you have" additional factor authentication.

Leo: I use it on Battle.Net. I use it wherever it works. So Blizzard has one, and they have an authenticator that you have to download another app on your phone, and it gives you the one-time key, and you'd use the password...

Steve: Mine is never far from me.

Leo: Yup, I've got my fob for PayPal. Although, as you point out, PayPal's got that little thing saying, "Did you lose your fob? Well, let's help you get in." So how good can this really be? And by the way, using LastPass would not have saved Mat in the least. It wasn't an issue of somebody stealing his passwords.

Steve: Nope.

Leo: And that's the key to this is that there are holes, it turns out, in all sorts of places. And it just takes somebody who's willing to kind of mess around...

Steve: And work the system.

Leo: ...and work the system. And that's what these kids are good at. They've got a lot of time. They're smart. And they're motivated, apparently.

Steve: And there's a culture. They're passing...

Leo: There's a culture. They pass this stuff around, exactly.

Steve: Exactly.

Leo: So I asked this guy, "How did you get started? Where did you learn this stuff? How did you get all these techniques?" He said, "I started when it was 16, and I wanted a cool gamer tag on Xbox 360. And I asked my friends." And, see, this is what happens. They start passing around techniques for hacking. And I doubt very much that these guys came up with their own techniques. Maybe they did. But I think in most cases they're just - it's like a recipe book.

Steve: There is an underground.

Leo: Step 1: Call Amazon. There's an underground.

Steve: Yep. And they're chatting, if they're in high school, I guess they're around that age, they're sitting around at lunch, passing back and forth new ways someone has found for running a scam. It's like, hey, I tried this, and this worked. And the person who comes up with it might be too timid to do it, but he tells somebody who's brazen enough to go give it a shot, to get on the phone and call Amazon and Apple.

Leo: There's no harm to doing that. They could say, well, if they get suspicious, you hang up and move on.

Steve: You've got to wonder, too, how anonymous those calls were. It's not as easy to obscure your phone number as it is your Internet connection.

Leo: Oh, yeah, it is.

Steve: Oh.

Leo: Oh, yeah, it is.

Steve: Okay.

Leo: But let's not go into that.

Steve: Okay.

Leo: Steve, this is such a good subject. It's a fascinating topic, and I'm really glad you addressed it. I guess we'll do questions next week.

Steve: Yes, we will. We spend so much time talking about technology because that's where all of this comes from. But this was a perfect example of how technology can't save us, if the policies are in place and the systems are in place that allow this kind of scheme. This had nothing to do with how long the passwords were, as you said, or how many bits of crypto were in use. These guys cut right through all that and sent tweets out of Mat's Twitter account. So, wow.

Leo: Thank you, Steve Gibson. He's the man. Next week your questions; right? We're going to do Q&A?

Steve: Yup. Yes.

Leo: So go to GRC.com/feedback to ask those questions. While you're there, check out SpinRite, the world's finest hard drive maintenance and recovery utility. You might pick up a couple of freebies - Steve's got a lot of them - including Perfect Paper Passwords. You can just print out some passwords. They're perfect. They're paper. The Password Haystacks, which I use now all the time. See, this is the irony. I know I have very secure passwords. I'm not worried about my passwords anymore [clearing throat].

Steve: Yup.

Leo: Apparently that doesn't matter. All his stuff is available at GRC.com. We do this show every Wednesday, 11:00 a.m. Pacific, 2:00 p.m. Eastern time. That's 1800 UTC on TWiT.tv. Watch live. We love it if you do. I love to see the chat and the feedback, and I certainly would pay attention to it. But you can also catch it after the fact. We make on-demand versions available. Now, Steve does some unusual on-demand versions. He does a 16Kb version for the bandwidth-impaired. That's at GRC.com. He's also got transcripts, which is the ultimate in compact, ASCII text, baby. All of that, GRC.com. But for the video, the higher quality audio, we've got that at TWiT.tv/sn. Steve's on the Twitter...

Steve: Oh, and Leo?

Leo: Yeah.

Steve: I forgot to mention, I made an improvement to the little animation that you saw last week for the first time.

Leo: Steve was playing with his HTML5 and his JavaScript.

Steve: If you do GRC.com/animation.htm, I added peak detection to the output of the read amplifier. So it came out pretty cool.

Leo: This is - you're having fun with this, aren't you.

Steve: Yeah, I am. I've...

Leo: This is cool. This is all programmatically generated. None of it is graphics; right? You're just drawing lines and boxes and squares.

Steve: Yeah. And it's like, oh, I think it's less than - it's around 30K. And when those waveforms get into the write amplifier there, then it starts switching its polarity, which changes the direction of magnetism on the disk platter. Then the platter rotates over my little schematic. Then the read head picks up on it. And now here's...

Leo: Whoa.

Steve: We've detected the pulse, the peak of the waveform.

Leo: Peak detector. Peak detector. You are a crackup. Oh, what fun. And by the way, you can view source on this. He has not obfuscated the code. I'm learning JavaScript, inspired by you, and I'm looking at the code because it's very cool. Very, very cool.

Steve: Fun stuff.

Leo: Yeah. Thank you, Steve Gibson.

Steve: Okay, my friend.

Leo: Thank you, everybody, for being here. Steve's on the Twitter, @SGgrc. He doesn't follow people, but you can @ message him, and he reads those.

Steve: Yup, I do.

Leo: And he responds, too.

Steve: I do.

Leo: Thanks, Steve.

Steve: Thanks, Leo.

Leo: We'll talk again next week on Security Now!.