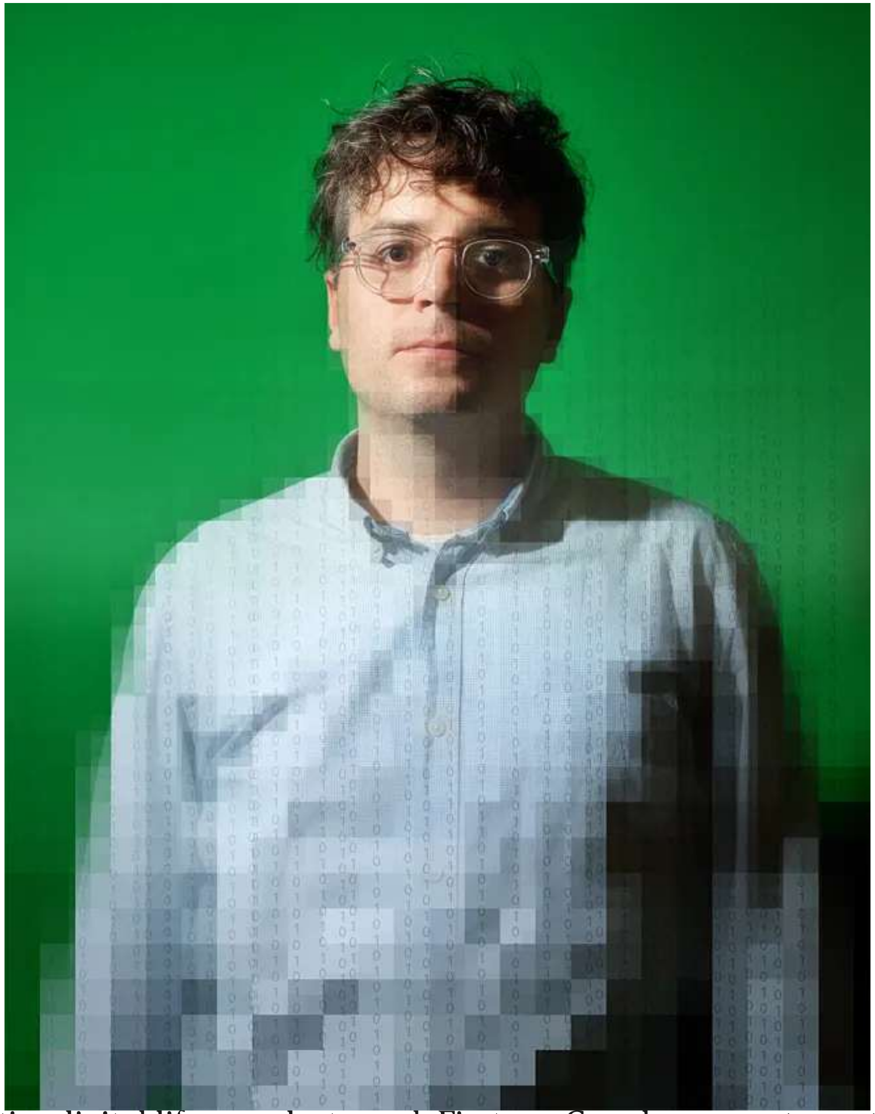
MAT HONAN GEAR 08.06.2012 08:01 PM

How Apple and Amazon Security Flaws Led to My Epic Hacking

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. Here's the story of exactly how my hackers created havoc by exploiting Apple and Amazon security flaws.



Meet Mat Honan. He just had his digital life dissolved by hackers. PHOTO: ARIEL ZAMBELICH/WIRED. ILLUSTRATION: ROSS PATTON/WIRED

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 AppleID 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 e-mails 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.

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.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 p.m. on Friday. 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.

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 tech support. 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.com e-mail – which, of course was my Me.com e-mail.

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.com e-mail, 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 e-mail to permanently reset my AppleID password.

At 4:52 p.m., a Gmail password recovery e-mail arrived in my me.com mailbox. Two minutes later, another e-mail 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.

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.com 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 AppleID is the associated e-mail 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. We are reviewing all of our processes for resetting account passwords to ensure our customers' data is protected."

On Monday, 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 e-mail 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.

By exploiting the customer service procedures employed by Apple and Amazon, hackers were able to get into iCloud and take over all of Mat Honan's digital devices – and data. *Photo: Ariel Zambelich/Wired*

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 Apple email 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 occurred. At this point, I was assuming that my seven-digit alphanumeric AppleID password had been hacked by brute force. In the comments (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 e-mail 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:

“didnt guess ur password or use bruteforce. 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? 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 fuck shit up, and watch it burn. It wasn’t personal.

“I honestly didn’t have any heat towards you before this. i just liked your username like I said before” he told me via Twitter Direct Message.

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 e-mail 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 e-mail 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 e-mail address, or had used two-factor authentication for Gmail, everything would have stopped here. But using that Apple-run me.com e-mail account as a backup meant told the hacker I had an AppleID account, which meant I was vulnerable to being hacked.

Be careful with your Amazon account – or someone might buy merchandise on your credit card, but send it to their home.
PHOTO: LUXURYLUKE/FLICKR

“You honestly can get into any email associated with apple,” Phobia claimed in an e-mail. And while it's work, that seems to be largely true.

Since he already had the e-mail, all he needed was my billing address and the last four digits of my credit card number to have Apple's 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 tricker, but it also relies on taking advantage of a company's back-end systems. Phobia says that a partner 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 account. All you need is the name on the account, an associated e-mail address, and the billing address. Amazon then allows you to input a new credit card. (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 will allow you to add a new e-mail address to the account. From here, you go to the Amazon website, and send a password reset to the new e-mail 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 by press time.

And it's also worth noting that one wouldn't have to call Amazon to pull this off. Your pizza guy could do the same thing, for example. If you have an AppleID, 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 e-mail 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. As Ed Bott pointed out on TWiT.tv, 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, 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 e-mail prefix across multiple accounts – 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 authentification is being considered.

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.

"yea i really am a nice guy idk 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 every1 can over come 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 wasnt the one that did it i feel sorry about that. Thats alot of memories im only 19 but if my parents lost and the footage of me and pics i would be beyond sad and im 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 AppleID, 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.

Additional reporting by Roberto Baldwin and Christina Bonnington. Portions of this story originally appeared on Mat Honan's Tumblr.

Continued: How I Resurrected My Digital Life After an Epic Hacking.

Mat Honan is a senior staff writer with WIRED. He lives in San Francisco.

SENIOR STAFF WRITER