MAT HONAN GEAR 08.17.2012 02:57 PM

Mat Honan: How I Resurrected My Digital Life After an Epic Hacking

After my accounts were hacked and my devices deleted, here's how I restored most of my data.

The team at DriveSavers who recovered data from a wiped MacBook Air laptop. From the left, John Christopher, Phillip Reynolds, Ron Powell, Angel Ortiz, and Joseph Novoa. Not pictured: Phil Baca. THE TEAM AT DRIVESAVERS WHO RECOVERED DATA FROM A WIPED MACBOOK AIR LAPTOP. FROM THE LEFT, JOHN CHRISTOPHER, PHILLIP REYNOLDS, RON POWELL, ANGEL ORTIZ, AND JOSEPH NOVOA. NOT PICTURED: PHIL BACA.

WHEN MY DATA died, it was the cloud that killed it. The triggers hackers used to break into my accounts and delete my files were all cloud-based services -- iCloud, Google, and Amazon. Some pundits have latched onto this detail to indict our era of cloud computing. Yet just as the cloud enabled my disaster, so too was it my salvation.

Yes, you can die by the cloud. But you can live by it too. Here's how I regained my digital life after it was taken away from me.

When hackers broke into my iCloud account and wiped my devices, my first assumption was that someone had broken into my local network. So the first thing I did was shut down the internet and turn off all of my other machines. I wanted those assholes out of my house. But that also meant I had no way to send or receive data.

AppleCare's phone support was useless. The 90 fruitless minutes I spent on the phone accomplished nothing at all to regain control of my AppleID. Nor did a follow-up help to stop the remote wipe taking over my MacBook Air. I had to get online. So to reconstruct my life, I started off by going next door, where I borrowed my neighbor's computer to use their internet.

Ultimately, I was able to get back into my iCloud account by resetting the password online. Once I did, I began restoring my iPhone and iPad from iCloud backups. The phone took seven hours to restore. The iPad took even longer. I could use neither during this time.

From my wife’s phone, I called my bank and completely changed my logins. Then I set about checking online to see which other accounts might have been compromised. By now I felt safe turning on our own home internet and using one of my other computers to check these accounts. But I hit an immediate problem: I didn’t know any of my passwords.

I'm a heavy 1Password user. I use it for everything. That means most of my passwords are long, alphanumeric strings of gibberish with random symbols. It's on my iPhone, iPad and Macbook. It syncs up across all those devices because I store the keychain in the cloud on Dropbox. Update a password on my phone, and the file is saved on Dropbox, where my computer will pull it down later, and vice versa.

But I didn't have it on any of our other systems. So now I couldn't get to my keychain. And so I was stuck in a catch-22. My Dropbox password was itself a 1password-generated litany of nonsense. Without access to Dropbox, I couldn't get my keychain. Without my keychain, I couldn't get into Dropbox.

And then I remembered that I had also used Dropbox previously on my wife's machine. Had I stored the password there?

Five hours after the hack started, still locked out of everything, I flipped open the lid of her computer, and nervously powered it up. And there it was: my Dropbox. And in it, my 1Password keychain, the gateway to my digital life.

It was time to get cranking. I set up a new Twitter account. And then, with my now-found password manager, I logged into Tumblr.

Here's the thing: I probably got my stuff back faster than you would have. I've been a technology journalist for more than a dozen years, and in that time I've made lots and lots of contacts. Meanwhile, my Tumblr post spread like warm butter across the piping hot English muffin of the internet.

A lot of people saw the post, some of whom were executives or engineers at Google and Twitter. I still had to go through official channels, but they pointed me to the right place to start the recovery process on both of those services. On Friday night, I filled out forms on both sites (Google's is here, Twitter's is here) to try to reclaim my accounts.

Someone else saw my posts on that night too: my hacker.

I had posited that the hackers had gotten in via brute forcing my 7-digit password. This caused my hacker, Phobia, to respond to me. No, he bragged, brute force wasn't involved. They got it right from AppleCare, he said via a Twitter DM. I still didn't know how that worked, exactly, but this piece of information led me to start digging.

As it turned out, breaking into Apple accounts was ridiculously easy. On Saturday, when I fully understood just how Phobia and his partner had gotten in (and how easily it could happen again), I made a distressed phone call to Apple to ask that the company lock everything down, and issue no more password resets.

It was on this call that I confirmed someone else had called in about my account at 4:33 p.m. the previous day -- someone who I now knew to be Phobia. Chandler McDonald, the tech who helped me on that call, was the first person at Apple to take what was happening really seriously, and was one of only two positive experiences I had with Apple that weekend (or since). McDonald reassured me that he was going to get my account locked down, and promised to call me the next day. And he did. I'm still grateful.

Also on Friday night, I began the process of restoring my Google account. Because I couldn't send a backup to my now non-functioning phone, I had to fill out some forms online that asked me questions about my account usage that, presumably, only I would know. For example, I was asked to name the five people I e-mailed the most.

On Saturday morning, I received an automated e-mail from Google asking me to go online and define even more personal information. This time, I was asked for things like the names of folders in my Gmail account, and the dates on which I had set up various other Google accounts, like Google Docs. It was a little flummoxing, and I wasn't sure I knew the answers to these questions. But I tried, and I guess I got the answers right.

That same day, while still waiting for access to my Google account, I was having another Google-related problem that was keeping me from being able to use my phone. Although the restore from backup was complete, and I could use over-the-air data

to access internet services, it would not send or receive calls. At first I couldn't understand why, and then realized it was because I had linked my number to Google Voice.

Since Google has integrated sign-ons across all accounts, not only was my Gmail nuked, but so was every other associated Google service as well. That meant my Google Voice number was dead. And because I (obviously) couldn't log into Google Voice, I couldn't opt to disconnect it from my phone. I called Sprint and asked the tech support rep there to do it for me. Done.

Almost immediately, my phone lit up with text messages from concerned friends, wanting to let me know I'd been hacked.

Thanks guys, I know. I know.

Just before noon on Saturday, my Google account was restored. Given what I've subsequently learned about how long it has taken others to do the same, I think that had my case not been escalated, this process could have taken 48 hours or more. Yes, I went through the normal steps, and had to prove I was who I claimed to be, but the process was likely faster for me than it would be for most.

Once in my inbox, I saw how remarkably little the intruders had done. They had torched the joint just after getting a password reset on Twitter. I went through and checked all my mail filters and settings to make sure new messages wouldn't be also copied to someone else without my knowledge, and systematically revoked every single app and website I'd authorized to connect to my Google account.

Saturday night, after verifying my Wired e-mail address and exchanging several e-mails with tech support, I got back into my Twitter account too. It was in ruins. There were racist and anti-gay tweets all over the place, as well as taunting remarks aimed at other hackers, and other users. At first I left these up, just as documentation, but then went in and deleted the worst of them.

That night, I stayed up late, direct-messaging Phobia on Twitter.

Sunday afternoon, I found myself at the Apple Store in San Francisco's worst mall. I was, to say the least, cranky. Although I'd called on a Friday night, the first appointment I could get was at 1 p.m. on Sunday. By 1:20 p.m., I was talking to an Apple genius named Max. He was awesome. He'd heard of my case.

He told me that while Apple couldn't recover my data, it could probably stop the wipe from progressing further. There was the 4-digit PIN that needed to be entered, as well as a firmware-level password, and I had neither. I told him all I cared about was preserving my data. He scurried away with my machine.

And indeed, Monday afternoon, Max called to let me know that they had been able to reset the firmware password. They couldn't crack the PIN, but he said I should be able to pull whatever data existed on there off. Good news. I began researching data-recovery firms.

A photo of the author and his daughter, shortly after her birth, that existed only on his hard drive. A PHOTO OF THE AUTHOR AND HIS DAUGHTER, SHORTLY AFTER HER BIRTH, THAT EXISTED ONLY ON HIS HARD DRIVE.

Getting data back from a SSD drive, like the one in my MacBook Air, is considerably trickier than recovering it from a standard HDD for all kinds of reasons -- from the way SSDs reallocate data, to the lack of a physical platter, to hardware-level encryption keys. I wasn't about to attempt to recover it myself. Max, my guy at the Apple Store, had suggested that I call DriveSavers. Several other people I know and respect, like TWiT's Leo Laporte, whose show I appeared on that weekend, told me the same thing.

And so, on Friday, exactly one week after my system was wiped, I sent my Mac away to Novato to see what could be recovered from the drive hackers had wiped.

In a nutshell, here's what happens when you take your machine to DriveSavers (and we'll have a full rundown on this later). First, they remove your drive from the machine and put it in a custom adapter. From there they use a proprietary method to image your system and copy that data to a secure "slicked" disk so there's no chance of data contamination. This is done extremely rapidly so that the original drive doesn't have to be powered up for very long.

Next they put the original drive aside to preserve it, and then begin working off the copy to see what's on there. In some cases, like mine, there are no more files or directory structures to pore over. So they scour the drives looking at raw hex data. When you see this in action, it looks a lot like *The Matrix*, with rows and rows of random numbers and characters scrolling up a screen, faster than your eyes can focus on.

Except, that's not what they saw on mine.

When Drivesavers began looking at my machine, the first 6GB of data held a clean install of Mac OS X. And after that, all they saw was row after row after row of zeroes. That data had been zeroed out. Overwritten. No recovery.

And then numbers. That beautiful hex data started rolling across the screen. Yes, 25 percent of my drive was gone and beyond repair. But the remaining 75 percent? Hope for life. DriveSavers called me to come look at what they had found, and my wife and I drove up there on Wednesday morning.

My data came back to me on an external hard drive, organized by file types. The thing I cared most about, above all else, was my photo library. And there, in a folder full of JPGs, was photo after photo after photo that I had feared were gone forever. Subfolders were organized by the year, month and day files were created. I went immediately to the folder that bore the date my daughter was born. They were there. Everything was there. We were floored. I nearly cried.

I am an over-sharer. But the things most intimate in life, I tend to keep private. And so although I have posted picture after picture to Flickr, Facebook and Instagram, the stuff that was really important -- the stuff that maybe even was most important -- has always been mine alone. It lived nowhere but on my hard drive.

Some of the photos were ancient artifacts that traveled with me from machine to machine with each upgrade cycle. In fact, much of the data was far older than the last device it was stored on. Most of those older images had been backed up to an external hard drive. And some of the newer ones were safe on PhotoStream, one of Apple's iCloud services. But most of the shots that I had taken with my camera over the past 20 months since I last backed up were lost forever. And here they were again, recovered. Reborn. It was gorgeous.

I didn't get everything back. DriveSavers was only looking for the things I specifically requested. I've lost all my applications, for example, as well as long-established preferences and settings that have been moving from machine to machine with me. But that's OK. I can live without them. I can buy them again. Whatever. Besides, sometimes it's nice to start with a clean slate, and I spent yesterday installing a new, clean operating system on my MacBook Air.

The bottom line is that I have all my photos and all the home movies I've shot. Every one of them. And seemingly all of my most important documents as well. That felt like a miracle.

The bill for all this? $1,690. Data doesn't come cheap.

I've been asked again and again what I've learned, and what I now do differently. I'm still figuring some of that out.

I'm certainly a backup believer now. When you control your data locally, and have it stored redundantly, no one can take it from you. Not permanently, at least. I've now got a local and online backup solution, and I'm about to add a second off-site backup into that mix. That means I'll have four copies of everything important to me. Overkill? Probably. But I'm once bitten.

And then there's the cloud. I'm a bigger believer in cloud services than ever before. Because I use Rdio, not iTunes, I had all my music right away. Because I use Evernote to take reporting notes, everything that I was currently working on still existed. Dropbox and 1Password re-opened every door for me in a way that would have been impossible if I were just storing passwords locally via my browser.

But I'm also a security convert.

It's shameful that Apple has asked its users to put so much trust in its cloud services, and not put better security mechanisms in place to protect them. AppleIDs are too easily reset, which effectively makes iCloud a data security nightmare. I've had person after person after person report similar instances to me, some providing documentation showing how easily their Apple accounts were compromised.

And due to Apple's opacity, I have no way of knowing if things have improved. Apple has refused to tell me in what ways its policies weren't followed "completely" in my case. Despite being an Apple user for nearly 20 years and having generally positive feelings toward the company, I no longer trust it to do the right thing in terms of protecting my data. I've turned off its Find My services and won't turn them back on.

Amazon also had a glaring security flaw, and although it has fixed that exploit, the flaw's mere existence should serve as a warning to all of us about all of our other accounts. We don't often know what's required to issue a password reset, or have someone get into our account through a company's tech support system.

But hackers do.

I'm working on another story looking at how widespread these practices are, and while there's much reporting left to be done, it's already very clear that the vulnerabilities at Amazon aren't unique. It's also clear that many of these gaping security holes are common knowledge within certain communities online. Bored teenagers up late on hot summer nights know more about social engineering exploits than I would wager most of the executives at affected companies do. That needs to change.

Previously, when I had the option for ease-of-use versus security, I always went the easy route. I stored my credit cards with the merchants I used for faster transactions. I didn't enable two-factor authentication on Google or Facebook. I never set up dedicated (and secret) e-mail accounts for password management. I take those steps now. But I also know that no matter what security measures I take, they can all be undone by factors beyond my control.

We don't own our account security. And as more information about us lives online in ever more locations, we have to make sure that those we entrust it with have taken the necessary steps to keep us safe. That's not happening now. And until it does, what happened to me could happen to you.

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

SENIOR STAFF WRITER