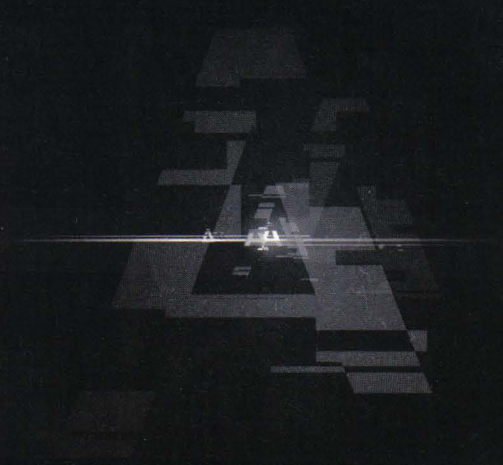
They took my photos,

my email,

my files.

H  C

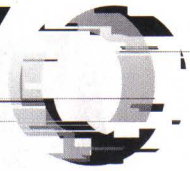
Passwords have failed.
It's time to try something new.

BY MAT HONAN

PHOTOGRAPHS BY ETHAN HILL


KED

YOU HAVE THAT CAN YOUR



IT'S NOT A WELL-KEPT SECRET, EITHER. Just a simple string of characters—maybe six of them if you're careless, 16 if you're cautious—that can reveal everything about you.

Your email. Your bank account. Your address and credit card number. Photos of your kids or, worse, of yourself, naked. The precise location where you're sitting right now as you read these words. Since the dawn of the information age, we've bought into the idea that a password, so long as it's elaborate enough, is an adequate means of protecting all this precious data. But in 2012 that's a fallacy, a fantasy, an outdated sales pitch. And anyone who still mouths it is a sucker—or someone who takes *you* for one.

No matter how complex, no matter how unique, your passwords can no longer protect you.

Look around. Leaks and dumps—hackers breaking into computer systems and releasing lists of usernames and passwords on the open web—are now regular occurrences. The way we daisy-chain accounts, with our email address doubling as a universal username, creates a single point of failure that can be exploited with devastating results. Thanks to an explosion of personal information being stored in the cloud, tricking customer service agents into resetting passwords has never been easier. All a hacker has to do is use personal information that's publicly available on one service to gain entry into another.

This summer, hackers destroyed my entire digital life in the span of an hour. My Apple, Twitter, and Gmail passwords were all robust—seven, 10, and 19 characters, respectively, all alphanumeric, some with symbols thrown in as well—but the three accounts were linked, so once the hackers had conned their way into one, they had them all. They really just wanted my Twitter handle: @mat. As a three-letter username, it's considered prestigious. And to delay me from getting it back, they used my Apple account to wipe every one of my devices, my iPhone and iPad and MacBook, deleting all my messages and documents and every picture I'd ever taken of my 18-month-old daughter.

Since that awful day, I've devoted myself to researching the world of online security. And what I have found is utterly terrifying. Our digital lives are simply too easy to crack. Imagine that I want to get into your email. Let's say you're on AOL. All I need to do is go to the website and supply your name plus maybe the city you were born in, info that's easy to find in the age of Google. With that, AOL gives me a password reset, and I can log in as you.

First thing I do? Search for the word "bank" to figure out where you do your online banking. I go there and click on the Forgot Password? link. I get the password reset and log in to your account, which I control. Now I own your checking account as well as your email.

MAT HONAN (@mat) *is a senior writer* [redacted]

SANDRA GARCIA

A PASSWORD HACKER IN ACTION

The following is from a January 2012 live chat between Apple online support and a hacker posing as Brian—a real Apple customer. The hacker's goal: resetting the password and taking over the account.

APPLE: Can you answer a question from the account? Name of your best friend?

HACKER: I think that is "Kevin" or "Austin" or "Max."

APPLE: None of those answers are correct. Do you think you may have entered last names with the answer?

HACKER: I might have, but I don't think so. I've provided the last 4, is that not enough?

APPLE: The last four of the card are incorrect. Do you have another card?

HACKER: Can you check again? I'm looking at my Visa here, the last 4 is "5555."

APPLE: Yes, I have checked again. 5555 is not what is on the account. Did you try to reset online and choose email authentication?

HACKER: Yes, but my email has been hacked. I think the hacker added a credit card to the account, as many of my accounts had the same thing happen to them.

APPLE: You want to try the first and last name for the best friend question?

HACKER: Be right back. The chicken is burning, sorry. One second.

APPLE: OK.

HACKER: Here, I'm back. I think the answer might be Chris? He's a good friend.

APPLE: I am sorry, Brian, but that answer is incorrect.

HACKER: Christopher Aylsworth is the full name. Another possibility is Raymond McAlister.

APPLE: Both of those are incorrect as well.

HACKER: I'm just gonna list off some friends that might be haha. Brian Coca. Bryan Yount. Steven May.

APPLE: How about this. Give me the name of one of your custom mail folders.

HACKER: "Google" "Gmail" "Apple" I think. I'm a programmer at Google.

APPLE: OK, "Apple" is correct. Can I have an alternate email address for you?

HACKER: The alternate email I used when I made the account?

APPLE: I will need an email address to send you the password reset.

HACKER: Can you send it to "toe@aol.com"?

APPLE: The email has been sent.

HACKER: Thanks!

[redacted]

PASSWORDS ARE AS OLD as civilization. And for as long as they've existed, people have been breaking them.

In 413 BC, at the height of the Peloponnesian War, the Athenian general Demosthenes landed in Sicily with 5,000 soldiers to assist in the attack on Syracusae. Things were looking good for the Greeks. Syracusae, a key ally of Sparta, seemed sure to fall.

But during a chaotic nighttime battle at Epipole, Demosthenes' forces were scattered, and while attempting to regroup they began calling out their watchword, a prearranged term that would identify soldiers as friendly. The Syracusans picked up on the code and passed it quietly through their ranks. At times when the Greeks looked too formidable, the watchword allowed their opponents to pose as allies. Employing this ruse, the undermatched Syracusans decimated the invaders, and when the sun rose, their cavalry mopped up the rest. It was a turning point in the war.

The first computers to use passwords were likely those in MIT's Compatible Time-Sharing System, developed in 1961. To limit the time any one user could spend on the system, CTSS used a login to ration access. It only took until 1962 when a PhD student named Allan Scherr, wanting more than his four-hour allotment, defeated the login with a simple hack: He located the file containing the passwords and printed out all of them. After that, he got as much time as he wanted.

During the formative years of the web, as we all went online, passwords worked pretty well. This was due largely to how little data they actually needed to protect. Our passwords were limited to a handful of applications: an ISP for email and maybe an ecommerce site or two. Because almost no personal information was in the cloud—the cloud was barely a wisp at that point—there was little payoff for breaking into an individual's accounts; the serious hackers were still going after big corporate systems.

So we were lulled into complacency. Email addresses morphed into a sort of universal login, serving as our username just about everywhere. This practice persisted even as the number of accounts—the number of failure points—grew exponentially. Web-based email was the gateway to a new slate of cloud apps. We began banking in the cloud, tracking our finances in the cloud, and doing our taxes in the cloud. We stashed our photos, our documents, our data in the cloud.

Matthew Prince protected his Google Apps account with a second code that would be sent to his phone—so the hackers got his cell account.

Eventually, as the number of epic hacks increased, we started to lean on a curious psychological crutch: the notion of the "strong" password. It's the compromise that growing web companies came up with to keep people signing up and entrusting data to their sites. It's the Band-Aid that's now being washed away in a river of blood.

Every security framework needs to make two major trade-offs to function in the real world. The first is convenience: The most secure system isn't any good if it's a total pain to access. Requiring you to remember a 256-character hexadecimal password might keep your data safe, but you're no more likely to get into your account than anyone else. Better security is easy if you're willing to greatly inconvenience users, but that's not a workable compromise.

HOW TO SURVIVE THE PASSWORD APOCALYPSE

Until we figure out a better system for protecting our stuff online, here are four mistakes you should never make—and four moves that will make your accounts harder (but not impossible) to crack. —*M.H.*

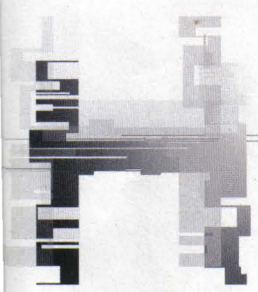
DON'T

- **REUSE PASSWORDS.** If you do, a hacker who gets just one of your accounts will own them all.
- **USE A DICTIONARY WORD AS YOUR PASSWORD.** If you must, then string several together into a pass phrase.
- **USE STANDARD NUMBER SUBSTITUTIONS.** Think "P455w0rd" is a good password? N0p3! Cracking tools now have those built in.
- **USE A SHORT PASSWORD**—no matter how weird. Today's processing speeds mean that even passwords like "h6!r$q" are quickly crackable. Your best defense is the longest possible password.

The second trade-off is privacy. If the whole system is designed to keep data secret, users will hardly stand for a security regime that shreds their privacy in the process. Imagine a miracle safe for your bedroom: It doesn't need a key or a password. That's because security techs are in the room, watching it 24/7, and they unlock the safe whenever they see that it's you. Not exactly ideal. Without privacy, we could have perfect security, but no one would accept a system like that.

For decades now, web companies have been terrified by both trade-offs. They have wanted the act of signing up and using their service to seem both totally private and perfectly simple—the very state of affairs that makes adequate security impossible. So they've settled on the strong password as the cure. Make it long enough, throw in some caps and numbers, tack on an exclamation point, and everything will be fine.

But for years it hasn't been fine. In the age of the algorithm, when our laptops pack more processing power than a high-end workstation did a decade ago, cracking a long password with brute force computation takes just a few million extra cycles. That's not even counting the new hacking techniques that simply steal our passwords or bypass them entirely—techniques that no password length or complexity can ever prevent. The number of data breaches in the US increased by 67 percent in 2011, and each major breach is enormously expensive: After Sony's PlayStation account database was hacked in 2011, the company had to shell out $171 million to rebuild its network and protect users from identity theft. Add up the total cost, including lost business, and a single hack can become a billion-dollar catastrophe.



HOW DO OUR ONLINE PASSWORDS fall? In every imaginable way: They're guessed, lifted from a password dump, cracked by brute force, stolen with a keylogger, or reset completely by conning a company's customer support department.

Let's start with the simplest hack: guessing. Carelessness, it turns out, is the biggest security risk of all. Despite years of being told not to, people still use lousy, predictable passwords. When security consultant Mark Burnett compiled a list of the 10,000 most common passwords based on easily available sources (like passwords dumped online by hackers and simple Google searches), he found the number one password people used was, yes, "password." The second most popular? The number 123456. If you use a dumb password like that, getting into your account is trivial. Free software tools with names like Cain and Abel or John the Ripper automate password-cracking to such an extent that, very literally, any idiot can do it. All you need is an Internet connection and a list of common passwords—which, not coincidentally, are readily available online, often in database-friendly formats.

What's shocking isn't that people still use such terrible passwords. It's that some companies continue to allow it. The same lists that can be used to crack passwords can also be used to make sure no one is able to choose those passwords in the first place. But saving us from our bad habits isn't nearly enough to salvage the password as a security mechanism.

Our other common mistake is password reuse. During the past two years, more than 280 million "hashes" (i.e., encrypted but readily crackable pass-

DO

- **ENABLE TWO-FACTOR AUTHENTICATION WHEN OFFERED.** When you log in from a strange location, a system like this will send you a text message with a code to confirm. Yes, that can be cracked, but it's better than nothing.

- **GIVE BOGUS ANSWERS TO SECURITY QUESTIONS.** Think of them as a secondary password. Just keep your answers memorable. My first car? Why, it was a "Camper Van Beethoven Freaking Rules."

- **SCRUB YOUR ONLINE PRESENCE.** One of the easiest ways to hack into an account is through your email and billing address information. Sites like Spokeo and WhitePages.com offer opt-out mechanisms to get your information removed from their databases.

- **USE A UNIQUE, SECURE EMAIL ADDRESS FOR PASSWORD RECOVERIES.** If a hacker knows where your password reset goes, that's a line of attack. So create a special account you never use for communications. And make sure to choose a username that isn't tied to your name—like m****n@wired.com—so it can't be easily guessed.

words) have been dumped online for everyone to see. LinkedIn, Yahoo, Gawker, and eHarmony all had security breaches in which the usernames and passwords of millions of people were stolen and then dropped on the open web. A comparison of two dumps found that 49 percent of people had reused usernames and passwords between the hacked sites.

"Password reuse is what really kills you," says Diana Smetters, a software engineer at Google who works on authentication systems. "There is a very efficient economy for exchanging that information." Often the hackers who dump the lists on the web are, relatively speaking, the good guys. The bad guys are stealing the passwords and selling them quietly on the black market. Your login may have already been compromised, and you might not know it—until that account, or another that you use the same credentials for, is destroyed.

Hackers also get our passwords through trickery. The most well-known technique is phishing, which involves mimicking a familiar site and asking users to enter their login information. Steven Downey, CTO of Shipley Energy in Pennsylvania, described how this technique compromised the online account of one of his company's board members this past spring. The executive had used a complex alphanumeric password to protect her AOL email. But you don't need to crack a password if you can persuade its owner to give it to you freely.

The hacker phished his way in: He sent her an email that linked to a bogus AOL page, which asked for her password. She entered it. After that he did nothing. At first, that is. The hacker just lurked, reading all her messages and getting to know her. He learned where she banked and that she had an accountant who handled her finances. He even learned her electronic mannerisms, the phrases and salutations she used. Only then did he pose as her and send an email to her accountant, ordering three separate wire transfers totaling roughly $120,000 to a bank in Australia. Her bank at home sent $89,000 before the scam was detected.

An even more sinister means of stealing passwords is to use malware: hidden programs that burrow into your computer and secretly send your data to other people. According to a Verizon report, malware attacks accounted for 69 percent of data breaches in 2011. They are epidemic on Windows and, increasingly, Android. Malware works most commonly by installing a keylogger or some other form of spyware that watches what you type or see. Its targets are often large organizations, where the goal is not to steal one password or a thousand passwords but to access an entire system.

One devastating example is ZeuS, a piece of malware that first appeared in 2007. Clicking a rogue link, usually from a phishing email, installs it on your computer. Then, like a good human hacker, it sits and waits for you to log in to an online banking account somewhere. As soon as you do, ZeuS grabs your password and sends it back to a server accessible to the hacker. In a single case in 2010, the FBI helped apprehend five individuals in the Ukraine who had employed ZeuS to steal $70 million from 390 victims, primarily small businesses in the US.

Targeting such companies is actually typical. "Hackers are increasingly going after small businesses," says Jeremy Grant, who runs the Department of Commerce's National Strategy for Trusted Identities in Cyberspace. Essentially, he's the guy in charge of figuring out how to get us past the current password regime. "They have more money than individuals and less protection than large corporations."

IF OUR PROBLEMS WITH PASSWORDS ended there, we could probably save the system. We could ban dumb passwords and discourage reuse. We could train people to outsmart phishing attempts. (Just look closely at the URL of any site that asks for a password.) We could use antivirus software to root out malware.

But we'd be left with the | CONTINUED ON PAGE 220

Hacked

CONTINUED FROM PAGE 187

weakest link of all: human memory. Passwords need to be hard in order not to be routinely cracked or guessed. So if your password is any good at all, there's a very good chance you'll forget it—especially if you follow the prevailing wisdom and don't write it down. Because of that, every password-based system needs a mechanism to reset your account. And the inevitable trade-offs (security versus privacy versus convenience) mean that recovering a forgotten password can't be too onerous. That's precisely what opens your account to being easily overtaken via social engineering. Although "socialing" was responsible for just 7 percent of the hacking cases that government agencies tracked last year, it raked in 37 percent of the total data stolen.

Socialing is how my Apple ID was stolen this past summer. The hackers persuaded Apple to reset my password by calling with details about my address and the last four digits of my credit card. Because I had designated my Apple mailbox as a backup address for my Gmail account, the hackers could reset that too, deleting my entire account—eight years' worth of email and documents—in the process. They also posed as me on Twitter and posted racist and antigay diatribes there.

After my story set off a wave of publicity, Apple changed its practices: It temporarily quit issuing password resets over the phone. But you could still get one online. And so a month later, a different exploit was used against *New York Times* technology columnist David Pogue. This time the hackers were able to reset his password online by getting past his "security questions."

You know the drill. To reset a lost login, you need to supply answers to questions that (supposedly) only you know. For his Apple ID, Pogue had picked (1) What was your first car? (2) What is your favorite model of car? and (3) Where were you on January 1, 2000? Answers to the first two were available on Google: He had written that a Corolla had been his first car, and had recently sung the praises of his Toyota Prius. The hackers just took a wild guess on the third question. It turns out that at the dawn of the new millennium, David Pogue, like the rest of the world, was at a "party."

With that, the hackers were in. They dove into his address book (he's pals with magician David Blaine!) and locked him out of his kitchen iMac.

OK, you might think, but that could never happen to me: David Pogue is Internet-famous, a prolific writer for the major media whose every brain wave goes online. But have you thought about your LinkedIn account? Your Facebook page? Your kids' pages or your friends' or family's? If you have a serious web presence, your answers to the standard questions—still often the only options available—are trivial to root out. Your mother's maiden name is on Ancestry.com, your high school mascot is on Classmates, your birthday is on Facebook, and so is your best friend's name—even if it takes a few tries.

The ultimate problem with the password is that it's a single point of failure, open to many avenues of attack. We can't possibly have a password-based security system that's memorable enough to allow mobile logins, nimble enough to vary from site to site, convenient enough to be easily reset, and yet also secure against brute-force hacking. But today that's exactly what we're banking on—literally.

WHO IS DOING THIS? Who wants to work that hard to destroy your life? The answer tends to break down into two groups, both of them equally scary: overseas syndicates and bored kids.

The syndicates are scary because they're efficient and wildly prolific. Malware and virus-writing used to be something hobbyist hackers did for fun, as proofs of concept. Not anymore. Sometime around the mid-2000s, organized crime took over. Today's virus writer is more likely to be a member of the professional criminal class operating out of the former Soviet Union than some kid in a Boston dorm room. There's a good reason for that: money.

Given the sums at stake—in 2011 Russian-speaking hackers alone took in roughly $4.5 billion from cybercrime—it's no wonder that the practice has become organized, industrialized, and even violent. Moreover, they are targeting not just businesses and financial institutions but individuals too. Russian cybercriminals, many of whom have ties to the traditional Russian mafia, took in tens of millions of dollars from individuals last year, largely by harvesting online banking passwords through phishing and malware schemes. In other words, when someone steals your Citibank password, there's a good chance it's the mob.

But teenagers are, if anything, scarier, because they're so innovative. The groups that hacked David Pogue and me shared a common member: a 14-year-old kid who goes by the handle "Dictate." He isn't a hacker in the traditional sense. He's just calling companies or chatting with them online and asking for password resets. But that does not make him any less effective. He and others like him start by looking for information about you that's publicly available: your name, email, and home address, for example, which are easy to get from sites like Spokeo and WhitePages.com. Then he uses that data to reset your password in places like Hulu and Netflix, where billing information, including the last four digits of your credit card number, is kept visibly on file. Once he has those four digits, he can get into AOL, Microsoft, and other crucial sites. Soon, through patience and trial and error, he'll have your email, your photos, your files—just as he had mine.

Why do kids like Dictate do it? Mostly just for lulz: to fuck shit up and watch it burn. One favorite goal is merely to piss off people by posting racist or otherwise offensive messages on their personal accounts. As Dictate explains, "Racism invokes a funnier reaction in people. Hacking, people don't care too much. When we jacked @jennarose3xo"—aka Jenna Rose, an unfortunate teen singer whose videos got widely hate-watched in 2010—"I got no reaction from just tweeting that I jacked her stuff. We got a reaction when we uploaded a video of some black guys and pretended to be them." Apparently, sociopathy sells.

A lot of these kids came out of the Xbox hacking scene, where the networked competition of gamers encouraged kids to learn cheats to get what they wanted. In particular they developed techniques to steal so-called OG (original gamer) tags—the

STORIES OF MEETING IS BELIEVING GOTOMEETING.COM INNOVATION

"I believe that ***GoToMeeting with HDFaces*** *is really that key driver for successful collaborations."*

Mindjet CMO
Jascha Kaykas-Wolff

Find out why businesses like Mindjet believe in the power of GoToMeeting — the extremely simple, extraordinarily powerful way to collaborate face to face in high-definition video. **Try it free today.**

meetingisbelieving.com
#meetingisbelieving

GoToMeeting
by CITRIX

back in the right sequence, and—presto.

None of this is to say that biometrics won't play a crucial role in future security systems. Devices might require a biometric confirmation just to use them. (Android phones can already pull this off, and given Apple's recent purchase of mobile-biometrics firm AuthenTec, it seems a safe bet that this is coming to iOS as well.) Those devices will then help to identify you: Your computer or a remote website you're trying to access will confirm a particular device. Already, then, you've verified something you are and something you have. But if you're logging in to your bank account from an entirely unlikely place—say, Lagos, Nigeria—then you may have to go through a few more steps. Maybe you'll have to speak a phrase into the microphone and match your voiceprint. Maybe your phone's camera snaps a picture of your face and sends it to three friends, one of whom has to confirm your identity before you can proceed.

In many ways, our data providers will learn to think somewhat like credit card companies do today: monitoring patterns to flag anomalies, then shutting down activity if it seems like fraud. "A lot of what you'll see is that sort of risk analytics," Grant says. "Providers will be able to see where you're logging in from, what kind of operating system you're using."

Google is already pushing in this direction, going beyond two-factor to examine each login and see how it relates to the previous one in terms of location, device, and other signals the company won't disclose. If it sees something aberrant, it will force a user to answer questions about the account. "If you can't pass those questions," Smetters says, "we'll send you a notification and tell you to change your password—because you've been owned."

The other thing that's clear about our future password system is which trade-off—convenience or privacy—we'll need to make. It's true that a multifactor system will involve some minor sacrifices in convenience as we jump through various hoops to access our accounts. But it will involve far more significant sacrifices in privacy. The security system will need to draw upon your location and habits, perhaps even your patterns of speech or your very DNA.

We need to make that trade-off, and eventually we will. The only way forward is real identity verification: to allow our movements and metrics to be tracked in all sorts of ways and to have those movements and metrics tied to our actual identity. We are not going to retreat from the cloud—to bring our photos and email back onto our hard drives. We live there now. So we need a system that makes use of what the cloud already knows: who we are and who we talk to, where we go and what we do there, what we own and what we look like, what we say and how we sound, and maybe even what we think.

That shift will involve significant investment and inconvenience, and it will likely make privacy advocates deeply wary. It sounds creepy. But the alternative is chaos and theft and yet more pleas from "friends" in London who have just been mugged. Times have changed. We've entrusted everything we have to a fundamentally broken system. The first step is to acknowledge that fact. The second is to fix it. ■