wired.com

Turns Out Your Complex Passwords Aren't That Much Safer

Robert McMillan

6–8 minutes

When the computer security company Hold Security reported that more than 1.2 billion online credentials had been swiped by Russian hackers, many people were worried---and justifiably so. Hold isn't saying exactly which websites were hit, but with so many credentials stolen, it's likely that hundreds of millions of ordinary consumers were affected.

Some of these may be incredibly complex passwords---with lots of jumbled numbers and symbols. And some may be incredibly simple---using just the simplest of English words, like, say,

"password." But after the hack, most all of them have left their users vulnerable to attack. According to Alex Holden, Hold Security's founder, the "vast majority" of the passwords he uncovered had been stored in plain text on company servers.

What this shows that a complex password isn't necessarily a secure password. As we've written before, password systems have a very annoying way of putting most of the hard work onto the shoulders of the users. You've got to mix up a jumble of numbers and letters (some in capitals, please) and special characters. Some passwords time-out after 90 days, forcing you to reset them. But that doesn't mean they're that much safer than simple passwords.

Some of our ideas about passwords date back to the 1980s, when the National Institute of Standards and Technology came up some guidelines for creating secure passwords for local area networks. Back then, they'd mail them out to interested computer security types via U.S. Post. Now, NIST is trying to help the U.S. move beyond the

password, says Donna Dodson NIST's chief cyber security advisor. "Putting the burden of security on the end-user and making it more complex just doesn't work," she says. "The security has to be usable for the end-user. Otherwise they're going to find workarounds."

>'Everyone is confused in this space. We don't know half of why we're doing this stuff.'

In some situations, a complex password can help you. But in others---like when the company holding your password stores it in plain text, without encrypting it---that complexity is meaningless. And some passwords may seem complex, when they're actually pretty easy to guess. They can trip you up, even if they're stored using cryptographic techniques, when someone hacks into the machines that they live on. The lesson here is that system administrators---the people who oversee all those password rules you have to follow---need to shoulder a bit more of the work. They need to better understand what makes a secure password---and how passwords should be stored.

"Everyone is confused in this space," says Cormac Herley, a Microsoft researcher who's been studying passwords for years. System administrators will lay down rules for passwords but often, "we don't know half of why we're doing this stuff.," says Herley. And they may not realize they should be spending their time securing systems in other ways.

Unsafe P@ssw0rds

That's why Herley, along with researchers at Microsoft and Ottawa's Carleton University, set out to to take a cold hard look at passwords and here's what they found: the way we traditionally measure password strength is inconsistent---and often say nothing about how hard it might be to guess a password.

Here's an example: some systems force you to chose an eight-character password, using capital letters, numbers and at least one number. That sounds pretty secure, but it's not. The word P@ssw0rd fits these criteria and password cracking tools such as JohntheRipper or hashcat will guess it in minutes. That's because they use

something called "mangling rules" which take dictionary words and substitute letters such as a for @ or s for $.

"The cracking software that's out there has known about all of these tricks for more than a decade," says Herley. "A lot of the password completion policies don't push people toward randomness and things that will pass 10^{14} guesses, they push people toward predictable strategies that will not."

Try out enough password-strength checkers, and you'll get the impression that more is always better when it comes to password. But that's not really the case, Herley says. Randomness is the key. But the problem---and it's a near-fatal one---is that humans are really, really bad at generating random passwords. So maybe we should just expect our passwords to suck, and concentrate on protecting accounts in other ways--like with two-factor authentication, where you have to use a password in tandem with something like a fingerprint, a text message, or a random number generated on a device you lug around.

What's more, system administrators need to spend more time securing the passwords they store. If sysadmins had been taking care of business before the Russian hack---locking down their websites and protecting their users passwords with cryptography instead of storing them in plain text---users would be a lot better off. "Rather than asking the end-user to do all the work---and there's actually not a lot of evidence that people will do the work---why don't we invest more effort on the system side by checking that we don't leak the password database?" says Paul van Oorschot, a computer science professor who did this research with the Microsoft team.

Some companies seem to get this. Amazon, for example, is ok with six-character passwords---no numbers or special characters required. Apple, on the other hand, forces you to run the gauntlet: capital letters, numbers, lower-case letters.

The way Herley and van Oorschot see things, some accounts are perfectly fine to have

completely low security. Using the word "password" as your throw-away password when you're forced to register to read an online news article may not be such a big deal. On the other hand, if you're using Gmail as your primary email account, you're going to make things more difficult. You want a password that's really hard to guess, and you want Google to text you a second password whenever you try to log in from a different device.

Either way, pinning your security on an insanely complex password is a fool's wager. Just ask the people running the airline, travel and social networking sites that got hacked by Alex Holden's Russian hackers. "Why are we burdening users with demands to chose stronger and stronger things with the goal of withstanding increasingly sophisticated guessing attacks when 1.2 billion credentials are just spewed from servers that are improperly protected," says Herley. "That seems like a big waste of effort."