A computer can guess more than 100,000,000,000 passwords per second. Still think yours is secure?

September 15 2020, by Paul Haskell-Dowland, Brianna O'shea

Credit: Paul Haskell-Dowland, Author provided

Passwords have been used for thousands of years, as a means of identifying ourselves to others and in more recent times, to computers. It's a simple concept—a shared piece of information, kept secret between individuals and used to "prove" identity.

Passwords in an IT context emerged in the 1960s with mainframe

computers (large centrally operated computers with remote "terminals" for user access). They're now used for everything from the PIN we enter at an ATM, to logging in to our computers and various websites.

But why do we need to "prove" our identity to the systems we access? And why are passwords so hard to get right?

What makes a good password?

Until relatively recently, a good password might have been a word or phrase of as little as six to eight characters. But we now have minimum length guidelines. Why? Because of "entropy."

When talking about passwords, entropy is the measure of predictability. The maths behind this isn't complex, but let's examine this with an even simpler measure: the number of possible passwords, sometimes referred to as the "password space."

If a one character password only contains one lowercase letter, there are only 26 possible passwords ("a" to "z"). By including uppercase letters, we increase our password space to 52 potential passwords.

Combination	Combinations per character	Example	Password Space
Lower case only	26	pass	456,976
Lower case only	26	password	208,827,064,576
Lower+upper case	52	Password	53,459,728,531,456
Lower+upper case + digits	62	Pa55w0rd	218,340,105,584,896
Lower+upper case + digits + symbols	92 (approx.)	Pa$$w0rd	5,132,188,731,375,616

Making a password longer or more complex greatly increases the potential 'password space'. More password space means a more secure password.

The password space continues to expand as the length is increased and other character types are added.

Looking at the above figures, it's easy to understand why we're encouraged to use long passwords with upper and lowercase letters, numbers and symbols. The more complex the password, the more attempts needed to guess it.

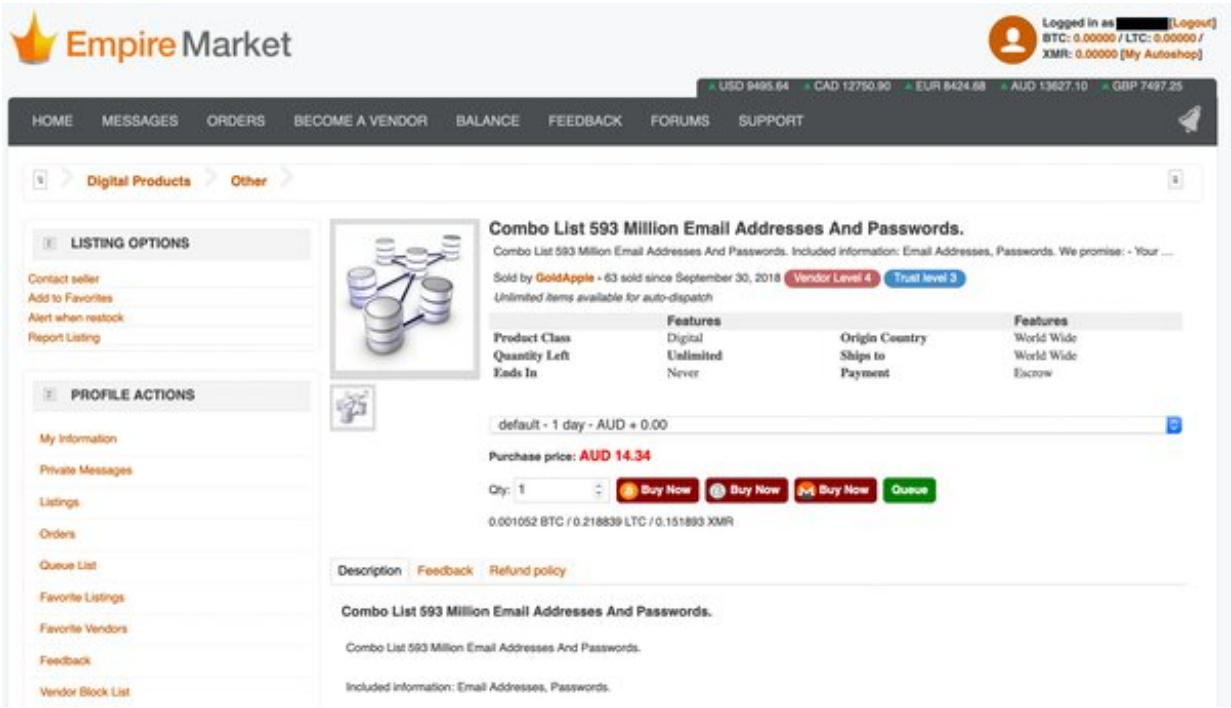
However, the problem with depending on password complexity is that computers are highly efficient at repeating tasks—including guessing passwords.

Last year, a record was set for a computer trying to generate every conceivable password. It achieved a rate faster than 100,000,000,000 guesses per second.

By leveraging this computing power, cyber criminals can hack into a system by bombarding it with as many password combinations as possible, in a process called brute force attacks.

And with cloud-based technology, guessing an eight-character password can be achieved in as little as 12 minutes and cost as little as US$25.

And because passwords are almost always used to give access to sensitive data or important systems, this motivates cyber criminals to actively seek them out. It also drives a lucrative market selling passwords, some of which come with email addresses and/or usernames.



You can purchase almost 600 million passwords online for just AU$14!

How are passwords stored on websites?

Website passwords are usually stored in a protected manner using a mathematical algorithm called hashing. A hashed password is unrecognizable and can't be turned back into the password (an irreversible process).

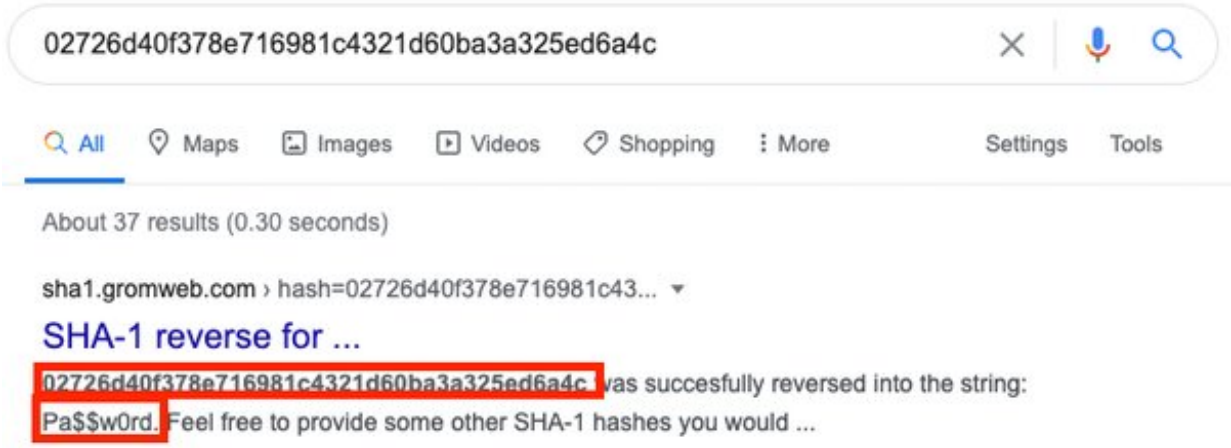
When you try to login, the password you enter is hashed using the same process and compared to the version stored on the site. This process is repeated each time you login.

For example, the password "Pa$$w0rd" is given the value "02726d40f378e716981c4321d60ba3a325ed6a4c" when calculated using the SHA1 hashing algorithm. Try it yourself.

When faced with a file full of hashed passwords, a brute force attack can be used, trying every combination of characters for a range of password lengths. This has become such common practice that there are websites that list common passwords alongside their (calculated) hashed value. You can simply search for the hash to potentially reveal the corresponding password.

The theft and selling of passwords lists is now so common, a dedicated website—haveibeenpwned.com—is available to help users check if their accounts are "in the wild." This has grown to include more than 10 billion account details.

If your email address is listed on this site you should definitely change the detected password, as well as on any other sites for which you use the same credentials.



This screenshot of a Google search result for the SHA hashed password value '02726d40f378e716981c4321d60ba3a325ed6a4c' reveals the original password: 'Pa$$w0rd'.

Is more complexity the solution?

You would think with so many password breaches occurring daily, we would have improved our password selection practices. Unfortunately, last year's annual SplashData password survey has shown little change over five years.

As computing capabilities increase, the solution would appear to be increased complexity. But as humans, we are not skilled at (nor motivated to) remember highly complex passwords.

We've also passed the point where we use only two or three systems needing a password. It's now common to access numerous sites, with each requiring a password (often of varying length and complexity). A recent survey suggests there are, on average, 70-80 passwords per person .

The good news is there are tools to address these issues. Most computers now support password storage in either the operating system or the web browser, usually with the option to share across multiple devices.

Examples include Apple's iCloud Keychain and the option to save passwords in Internet Explorer, Chrome and Firefox (although less reliable).

Rank	2015	2016	2017	2018	2019
1	123456	123456	123456	123456	123456
2	password	password	password	password	123456789
3	12345678	12345	12345678	123456789	qwerty
4	qwerty	12345678	qwerty	12345678	password
5	12345	football	12345	12345	1234567
6	123456789	qwerty	123456789	111111	12345678
7	football	1234567890	letmein	1234567	12345
8	1234	1234567	1234567	sunshine	iloveyou
9	1234567	princess	football	qwerty	111111
10	baseball	1234	iloveyou	iloveyou	123123

The 2019 annual SplashData password survey revealed the most common passwords from 2015 to 2019.

Password managers such as KeePassXC can help users generate long, complex passwords and store them in a secure location for when they're needed.

While this location still needs to be protected (usually with a long "master password"), using a password manager lets you have a unique, complex password for every website you visit.

This won't prevent a password from being stolen from a vulnerable website. But if it is stolen, you won't have to worry about changing the same password on all your other sites.

There are of course vulnerabilities in these solutions too, but perhaps that's a story for another day.

Commons license. Read the original article.

Provided by The Conversation