

# 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

---

```
, 4D9012B4A77A9524D675DAD27C3276AB5705E5E8:928060, 1411678A0B9E25EE2F7C8B2F7AC92B6A74B3F9C5
BC1682493351AD4FE8:775475, 48058E0C99BF7D689CE71C360699A14CE2F99774:741345, 42629D789C788D2
61, AB726600510D71831FB17A87A598EC755D6C3C74:727480, 05FE7461C607C33229772D402505601016A7D0
32DBB4420178F60CE321:684476, 48EFC4851E15940AF5D477D3C0CE99211A70A3BE:658945, 4BE30D9814C6E
8551, C53255317BB11707D0F614696B3CE6F221D0E2F2:642523, 74A871ACBF060DDA5FC7260D05A5924A34E4
C9E13CE848EF6FEAC81BFF:624152, BFE54CAA6D483CC3887DCE9D1B8EB91408F1EA7A:599177, 8F9F5C01D74
598193, 93EC71B22793A81569C94CA17E4D9C293D8E201F:592416, 31F2BFCCE79E11BDE1574CC1C9C8F97A71
56002641CFB067C9C94906A2:586071, BDDC5AD111CEF8744DDB460F32FF976BD09FD08B:584874, E1964A092
9:573736, F18CE40C9190C9A32A16EE0B1C8DD7013178445D:573297, 068CC94A2DBAD94C45FE95E5B2FEFC9F
F777C6EA07F9E05AB6CD8B38D7:572627, B7C40B9C66BC88D38A59E554C639D743E77F1B65:558726, DD2EDB8
1D5:557507, 5FA339BBB1EEACED3B52E54F44576AAF0D77D96:547528, 3ACD0BE86DE7DCCDBF91B20F94A68
316BE23842A5BCA7D69F29F69D77:513929, CB45C671CBC500627EA424EEA5F91996221B5935:510424, 88EA3
78392:505507, 775BB961B81DA1CA49217A48E533C832C337154A:489024, C60266A8ADAD2F8EE67D793B4FD3
9AE95CDDE6246BF4AA3FB058DD8373:452079, 3FCFC1F7F34E78A937E81171BA51DC39538DB993:442018, 782
08C9EBB:440413, 17B9E1C64588C7FA6419B4D29DC1F4426279BA01:434784, 2D27B62C597EC858F6E7B54E7E
9C691FA8ECE1FABCB8A6CEABFB5666B79:419377, 8D6E34F987851AA599257D3831A1AF040886842F:418052, F
A5477FDBB:401780, 043A558250409758B64F73D07D7F06B3DF654BC0:399592, 42849ADE74DE4722A85F06E8
529D87B5C318702BC1D7689F70B15EF4FC:389398, 3D0F3B9DDCACEC30C4008C5E030E6C13A478CB4F:376065
3FED15AB578:373547, 144D946202166F0C33C21FF3C24F967BFAAC126F:370783, FBA9F1C9AE2A8AFE7815C9
60370AD57D9BC3877E9024C507AB99303A64:369852, 7B21848AC9AF35BE0DDB2D6B9FC3851934DB8420:3657
664E5F4981862:365618, 1F5523A8F535289B3401B29958D01B2966ED61D2:360129, 7CE0359F12857F2A90C7
42A77AB7D4F51F59226CFAF891FCFB5B299B8:357376, D50B64AA30CF20FED0FA42FBCA5A64DF53ACE97A:35
```

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.

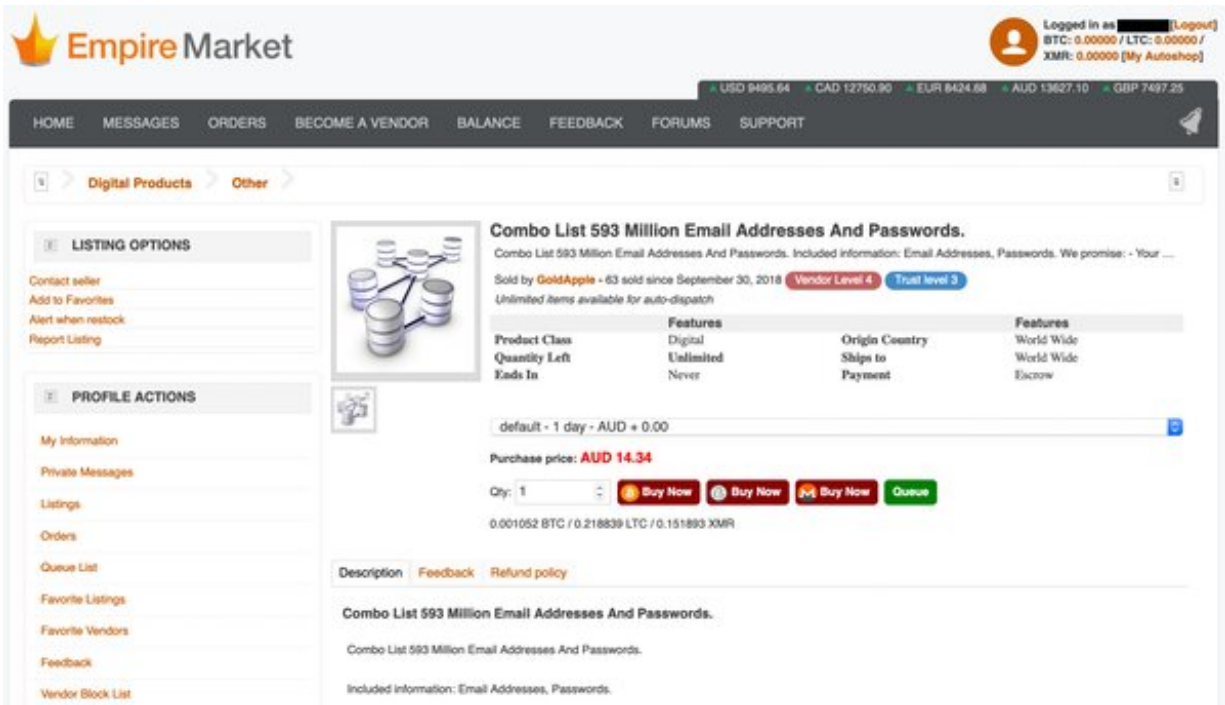
However, the problem with depending on password complexity is that computers are highly efficient at repeating tasks—including guessing passwords.

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.



The screenshot shows the Empire Market website interface. At the top, there's a navigation bar with links like HOME, MESSAGES, ORDERS, BECOME A VENDOR, BALANCE, FEEDBACK, FORUMS, and SUPPORT. A user is logged in as 'GoldApple' with a balance of 0.00000 BTC, 0.00000 LTC, and 0.00000 XMR. The main product listing is for 'Combo List 593 Million Email Addresses And Passwords' by GoldApple. The product is sold since September 30, 2018, and has a Vendor Level 4 and Trust level 3. The purchase price is AUD 14.34. The product features include Digital, Unlimited, and Never. The origin country is World Wide, and it ships to World Wide. The payment method is Escrow. The product is available for auto-dispatch. The purchase price is AUD 14.34. The quantity is 1. The buttons for 'Buy Now' and 'Queue' are visible. The product description is 'Combo List 593 Million Email Addresses And Passwords. Included information: Email Addresses, Passwords. We promise: - Your ...'. The product is sold since September 30, 2018, and has a Vendor Level 4 and Trust level 3. The purchase price is AUD 14.34. The quantity is 1. The buttons for 'Buy Now' and 'Queue' are visible. The product description is 'Combo List 593 Million Email Addresses And Passwords. Included information: Email Addresses, Passwords. We promise: - Your ...'.

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).

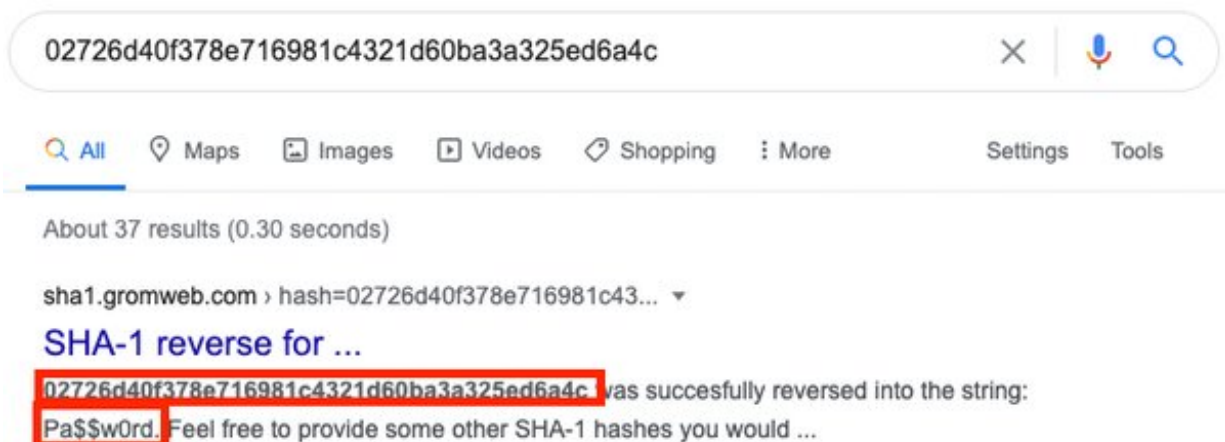
When you try to login, the password you enter is hashed using the same process and compared to the version stored on the site. This process is repeated each time you login.

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](https://haveibeenpwned.com)—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.

This article is republished from [The Conversation](#) under a Creative

Commons license. Read the [original article](#).

Provided by The Conversation

Citation: A computer can guess more than 100,000,000,000 passwords per second. Still think yours is secure? (2020, September 15) retrieved 3 May 2024 from <https://techxplore.com/news/2020-09-passwords.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.