Peterborough Fabian Society article

The Password Challenge!

The Password Challenge!

Most people use very inadequate passwords and so probably don't realise the nature and scale of the threat posed by password hackers – and how vulnerable they are to them.

Take this challenge to see how safe your online accounts are…

Imagine the questions listed below as a series of hurdles that you have to jump in order to show that your passwords are secure.

They relate to your important logons (ignoring banks with special security procedures).

These would include:

- Your email account (e.g. gmail, Yahoo, Outlook, Apple Mail)
- Social media sites (e.g. Facebook, Twitter, Linkedin)
- Sites which hold personal information about you
- Sites where you buy things and have personal or financial related information stored (e.g. Amazon, PayPal)
- Your blog sites

Answering "Yes" to any of them means you have failed to clear the hurdle and need to think again about what passwords you should use.

It's very rough, but I have tried to give the questions an order which will allow you to judge how good your defences are.

The questions

1 Are any of your passwords on this list? **1234**, **12345**, **123456**, **12345678**, **123456789**, **baseball**, **dragon**, **football**, **password**, **qwerty**

2 Are any of your passwords on this list? **111111**, **123123**, **1234567**, **696969**, **abc123**, **access**, **batman**, **letmein**, **master**, **michael**, **monkey**, **mustang**, **shadow**, **superman**, **trustno1**

3 Have you used the same password for all your sites?

4 Have you used your name or initials for any of your passwords?

5 Have you used the name of a relative or pet?

6 Are any of your passwords less than 7 characters long?

7 Have you used a lowercase name?

8 Have you used a name with just the first letter a capital?

9 Have you used a name?

10 Have you used the date of your anniversary/birthday? e.g. **05071998**

11 Have you used a number? e.g. **1835769**

12 Have you used a name or word followed by a number? e.g. **William2005**, **Ryan007**

13 Have you used a keyboard pattern? e.g.. **zxcvbnm**, **tgbyhnujm**

14 Have you used a name or word preceded by a number? e.g. **2456Allen**

15 Have you used a word that can be found in a dictionary (any dictionary, including Swahili)?

16 Have you used the same password on several of your websites?

17 Are any of your passwords less than 8 characters long?

18 Are any of your passwords written on a note left on or near your computer?

19 Have you used a name/number root password to generate individual passwords? e.g. **Rex123a, Rex123e, Rex123jl**

20 Have you used a name spelt backwards? e.g. **yelhsA**

21 Have you used a pronounceable string which is not in any dictionary? e.g. **glavondi**

22 Are any of your passwords less than 9 characters long with only lowercase characters?

23 Have you used a name and toggled the case of the characters (or maybe only the vowels/consonants)? e.g. **JoNaThAn, JoNaTHaN**

24 Have you used a word followed by a number and a special character? e.g. **Austin1!, Sports9?, Hiphop4$, Camels2%**

25 Have you duplicated a name or word? **SupermanSuperman**

26 Are any of your passwords less than 10 characters long with only lowercase characters?

27 Have you substituted numbers or symbols for letters? eg. **f00tb@ll, Hector8myiPh0ne**

28 Have you held down a special key to generate your password? e.g. ***ƒøø†∫å¬¬***

29 Have you used Steve Gibson's method? e.g. **Four4444....////**

30 Have you used a “Steve Gibson” root password to generate individual passwords? e.g. **Four4444....////a**, **Four4444....////b**, **Four4444....////c**

31 Have you used two, three or four words together? e.g. **HorseJumpFallOff**, **ChrisLovesFootball**, **CarJacketLadder**

32 Have you used the first letters of a common phrase, well known film, book, etc? e.g. **iwtbot,iwtwot**

33 Have you used five words together, but included names or well-used passwords? e.g. **jacktedgeorge1234dragon**

34 Have you used a common phrase from a book, film, TV series, song, etc.? e.g. **the force be with you**, **itwasthebestoftimes,itwastheworstoftimes**

35 Have you used a passphrase which is less than 20 characters long?

36 Have you used a passphrase which has a simple, grammatical format?

Well, how did you get on?

If you failed to clear the first dozen or so hurdles then I'm afraid you have to consider yourself easy meat for any self-respecting password hacker.

If you made it to the end unfazed, then congratulations! You have clearly thought carefully about your password security.

...... Or maybe you've just been lucky with the questions!

A password cracking program would ask much more searching ones.

As you may have already guessed, it's not just humans that you are up against!

Here's just one, small example of what any fairly sophisticated – now readily available – password cracking program is capable of doing:

> **This is a list of the 10,000 most frequently used passwords.**
>
> ***If yours is on it, then your password could be guessed in a heartbeat***
>
> ***and your account compromised in seconds.***

If you are skeptical of this claim, it's worth watching this 21 minute, 2016 video by Dr Mike Pound: Computerphile: Password Cracking *(skip the ads)*.

The DO's and DON'Ts of password security

This is my prescription for helping you towards a more secure online life.

My hope is that it is reasonably close to what experts think, but I appreciate that there may be a range of views and quibbles with some of the advice. And, of course, the rules are intended for the ordinary person – not for people with special expertise, who may have ways of dodging some of the bullets.

Password manager

DO get a password manager. *(All other options are either not very practical or leave you prey to hackers)*

1Password, Dashlane and LastPass are very good ones.

LastPass is a free one with lots of features.

There is a book by Joe Kissell which explains how to use **1Password** *(which I recommend getting)*.

DO take time to consider which one is best for you. *(Read this review)*

Think about: ease of use, synching between devices, sharing with your family, value for money.

DO make sure that it is backed up online. *(Your home computer may crash or be stolen)*

Your master password

DO create a very strong master password for your password manager. *(It's the key to all your other passwords)*

You must be able to remember it. *(Nobody can help you if you forget it)*

There are various ways you can do this.

I would suggest using a passphrase of at least 20 characters in length.

Use a phrase which is secret to you then insert a string of (say) 3 characters, which includes a number, an uppercase and a special character (e.g. $).

DON'T use anything which could be easily be found on the Internet e.g. in Wikipedia. *(Hackers could incorporate it into password crackers)*

DON'T use just a simple grammatical statement. *(It's more easily guessed by clever password crackers)*

DO make it easy to type. *(Consider the devices you will have to use it on)*

DO take your time about it. *(It could be a once in a life-time task).*

DO write your master password down and keep it safe. *(Consider telling someone about this).*

DON'T use your master password anywhere else. *(You don't know how securely it will be stored)*

Other passwords to remember

DO create a very strong password for your AppleId *(if you have one)*.

DO create a very strong password for computer, **if you have encrypted the hard drive**.

All the other passwords

DO let your password manager create all your other passwords. *(It's much better at it than you)*

Let it create 30+ character, random passwords with all the character types (if allowed).

DO use a different password for every account. *(Hackers try out stolen passwords on multiple sites)*

DON'T store your passwords in your browser. *(They are easily found by someone with access to your computer)*

DON'T **keep a separate record of your other passwords**. *(It defeats the point of having a password manager)*

Two-factor authentication

DO **use two-factor authentication if the account allows it**. *(It increases your security significantly)*

DO **make sure that you have another way of giving an authentication code**, should your primary method be unavailable. *(Plan for worst case scenarios)*

DO **print off any recovery codes and store them safely**. *(Your main device may not be available)*

Personal information

DON'T **use password hints for your accounts**. *(They can be stored insecurely and give hackers a head start)*

DON'T **answer security questions truthfully if you can avoid it**. (*Store your fibs in your password manager)*

DO **only give to social media sites the minimum of personal information** that could identify you or where you live. *(Fraudsters only need your name, address and date of birth to defraud you or steal your identity)*

DON'T **reveal your true birthday where it is not important to do so** (e.g. in social media sites).

Public places

DO **be careful in public places, especially when logging into important accounts**. (*Someone could be looking over your shoulder)*

DO **only use HTTPS secured websites to logon in public places**, especially cafés, airports, etc. (unless you are using VPN). (*Otherwise your communications could be picked up by criminals)*

DO **make sure your firewall is enabled before connecting to an open Wi-Fi hotspot**. *(Otherwise you could get infected by malware)*

DON'T **enter passwords into publicly available computers**. (*There could be a keylogger installed)*

DO **turn off the Wi-Fi on your phone or tablet when not in use**. *(It could automatically connect to a fake, malicious wi-fi hotspot)*

Malware

DO **make sure your firewall is switched on**. *(Otherwise malware will arrive in minutes)*

DO **install software updates as soon as you get them**. *(They are a signal to malware creators that there is a bug they might be able to exploit – but delay installing major updates of operating systems to avoid early bugs)*

DO **set your computer up to install updates automatically.** *(To avoid being caught out by Murphy's Law)*

DO **install anti-malware software**, even if you have a Mac. *(It's an important safeguard, but not infallible)*

DO **use a limited account for everyday tasks**. *(Malware that gains access to an admin account has free rein)*

DO **keep regular backups***. (It may be the only way to recover from malware like ransomware)*

DO **use a backup service that doesn't require any user intervention**. *(Otherwise Murphy's Law will find you out)*

DON'T **click on any links in emails unless you are certain that they are safe**. *(You can get malware just by visiting a website)*

DON'T **click on any email attachments unless you are certain they are safe**. *(You could download malware)*

DO **check downloads and attachments using your anti-malware software** if you are uncertain about them.

DON'T **reply to automated text or phone calls**. *(They could be smishing or vishing scams)*

DON'T **visit dubious websites**. (*You can be infected with malware just by visiting a web page)*

DO **be wary about clicking on adverts, even on legitimate websites**. *(They might be from criminals)*

DON'T **plug a “lost” USB into your computer**. *(It's a proven technique for spreading malware)*

DON'T install Flash or Java (different to JavaScript) unless you really need it. *(They both can be exploited by malware)*
DON'T download Android apps outside of Google Play *(The apps are more likely to contain malware)*

DON'T download iOS apps outside of Apple App Store (The apps may contain malware)

Some examples of how the number of combinations increase with password length

If your password was	(length)	**the number of possible combinations would be**	**this**
a	1		26
ab	2	26 x 26	676
aB	2	52 x 52	2,704
aBc	3	52 x 52 x 52	140,608
Ab1?	4	95 x 95 x 95 x 95	81,450,625
Ab1??	5	95 x 95 x 95 x 95 x 95	7,737,809,375
Ab1???	6	95 x 95 x 95 x 95 x 95 x 95	735,091,890,625
abcdefg	7	26 x 26 x 26 x 26 x 26 x 26 x 26	8,031,810,176

Tables

Table showing how password entropy increases

I've transformed the tables showing the maximum number of combinations that passwords of varying length would present to a password checker and the time it would take using 350 billion guesses a second to indicate how an entropy values relate to this.

Entropy of character combinations and the max. time it would take using 350 billion guesses a second

chars	**Lowercase only**		**Upper & lowercase**		**With numbers**		**With special characters**	
	bits	***max time***	**bits**	***max time***	**bits**	***max time***	**bits**	***max time***
1	5	*< 1 second*	6	*< 1 second*	6	*< 1 second*	7	*< 1 second*
2	9	*< 1 second*	11	*< 1 second*	12	*< 1 second*	13	*< 1 second*
3	14	*< 1 second*	17	*< 1 second*	18	*< 1 second*	20	*< 1 second*
4	19	*< 1 second*	23	*< 1 second*	24	*< 1 second*	26	*< 1 second*
5	60	*< 1 second*	29	*< 1 second*	30	*< 1 second*	33	*< 1 second*
6	28	*< 1 second*	34	*< 1 second*	36	*< 1 second*	39	2 seconds
7	33	*< 1 second*	40	3 seconds	41	10 seconds	46	3 minutes
8	38	*< 1 second*	46	2.5 minutes	48	10 minutes	53	5 hours
9	42	15 seconds	51	2 hours	54	11 hours	59	21 days
10	47	7 minutes	57	5 days	60	28 days	66	5 years
11	52	3 hours	63	8 months	66	5 years	72	515 years
12	56	3 days	68	35 years	71	292 years	79	48,956 years
13	61	3 months	74	1,841 years	77	18,122 years	85	5 million years
14	66	6 years	80	95,757 years	83	1 million years	92	442 million years
15	71	152 years	86	5 million years	89	70 million years	99	42 billion years

Note that the times shown are the **maximum** times that it would take the password cracker to find the password.

So, for example, an 8 character password like **97**A**4**E**vo**T has an entropy of 48 and the maximum time it would take to crack it would be 10 minutes.

It is possible that it might be cracked with the first guess, although the chances of that happening would be 62^8 or 218 trillion to 1 against. Likewise the possibility that it would take the maximum time would be the same.

As the time gets closer to 5 minutes, so the probably of the password being cracked increases.

There's a 50:50 chance that the password would be broken before 5 minutes.

Table showing how the number of combinations increase with length

Number of possible combinations for password lengths from 1 to 12 (trusting my maths!)

chars	Lowercase only	Upper & lowercase	With numbers	With special characters
1	26	52	62	95
2	676	2,704	3,844	9,025
3	17,576	140,608	238,328	857,375
4	456,976	7,311,616	14,776,336	81,450,625
5	11,881,376	380,204,032	916,132,832	7,737,809,375
6	308,915,776	19,770,609,664	56,800,235,584	735,091,890,625
7	8,031,810,176	1 trillion	3.5 trillion	69.8 trillion
8	208,827,064,576	53 trillion	218 trillion	6,634 trillion
9	5.4 trillion	2,780 trillion	13,537 trillion	630,249 trillion
10	141 trillion	144,555 trillion	839,299 trillion	59,873,693 trillion
11	3,670 trillion	7,516,865 trillion	52,036,561 trillion	5,688,000,922 trillion
12	95,428 trillion	390,877,006 trillion	3,226,266,762 trillion	540,360,087,662 trillion
13	2,481,152 trillion	20,325,604,337 trillion	200,028,539,268 trillion	51 septillion
14	64,509,974 trillion	1 septillion	12 septillion	4,876 septillion
15	1,677,259,342 trillion	54 septillion	768 septillion	46,3291 septillion

1 million = 1,000,000 = 10^6 1 billion = 1,000,000,000 = 10^9 1 trillion = 1,000,000,000,000 = 10^{12}

1 septillion = 1 trillion, trillion = 1,000,000,000,000,000,000,000,000 = 10^{24}

Table showing the time it would take to go through these combinations

Maximum time it would take to go through these combinations using 350 billion guesses a second

chars	Lowercase only	Upper & lowercase	With numbers	With special characters
1	*less than 1 second*	*less than 1 second*	*less than 1 second*	*less than 1 second*
2	*less than 1 second*	*less than 1 second*	*less than 1 second*	*less than 1 second*
3	*less than 1 second*	*less than 1 second*	*less than 1 second*	*less than 1 second*
4	*less than 1 second*	*less than 1 second*	*less than 1 second*	*less than 1 second*
5	*less than 1 second*	*less than 1 second*	*less than 1 second*	*less than 1 second*
6	*less than 1 second*	*less than 1 second*	*less than 1 second*	2 seconds
7	*less than 1 second*	3 seconds	10 seconds	3 minutes
8	*less than 1 second*	2.5 minutes	10 minutes	5 hours
9	15 seconds	2 hours	11 hours	21 days
10	7 minutes	5 days	28 days	5 years
11	3 hours	8 months	5 years	515 years
12	3 days	35 years	292 years	48,956 years
13	3 months	1,841 years	18,122 years	5 million years
14	6 years	95,757 years	1 million years	442 million years
15	152 years	5 million years	70 million years	42 billion years