The logic behind three random words

Whilst not a password panacea, using 'three random words' is still better than enforcing arbitrary complexity requirements.

Kate R

One of the most popular pages on the NCSC website, nearly 5 years after its first publication, is 'Three random words or #thinkrandom'. It explains how - by combining three random words - you can create a password that's 'random enough' to keep the bad guys out, but also 'easy enough' for you to remember.

In this blog, we're going to:

- explain why the NCSC continue to promote 'three random word' strategy (both at home and at work)
- respond to some concerns raised by NCSC customers who may be considering this strategy

---

The problems of complexity requirements

We've covered, at length, how enforcing complexity requirements is a poor defence against guessing attacks. Our minds struggle to remember random character strings, so we use predictable patterns (such as replacing the letter 'o' with a zero) to meet the required 'complexity' criteria.

Of course, attackers are familiar with these strategies and use this knowledge to optimise their attacks. Counter-intuitively, the enforcement of these complexity requirements results in the creation of more predictable passwords. Faced with making yet another password with specific requirements, users fall back on variations of something they already know and use, falsely believing it to be strong because it satisfies password strength meters (and is accepted by online services).

None of this is helped by:

1. Longstanding (and poor) advice that passwords have to be memorised, and storing them in *any* way (either in a password manager, a browser, or on a piece of paper) is risky.
2. The continued low uptake of password managers to both store and generate passwords (the NCSC has encouraged organisations and individuals to use password managers for some time now).

To be absolutely clear, there are a number of ways you **can** securely store your passwords, in a password manager, a browser, or on a piece of paper, so remembering them is no longer a problem*.

Why three random words?

The traditional password advice built around 'password complexity' failed because it told us to do things that most of us simply can't do (i.e. memorise lots of long, complex passwords).

Passwords generated from three random words help users to create unique passwords that are strong enough for many purposes, and can be remembered much more easily. This is also good for those who aren't aware of password managers, or are reluctant to use them. However, there are several other reasons why the NCSC chose the three random words strategy.

1 **Length**
Passwords made from multiple words will generally be longer than passwords made from a single word. Length is a common (and recommended) requirement for passwords, and promoting the use of a 'passphrase' created by combining words provides a way to achieve this without relying on predictable patterns (such as the addition of ! at the end of a password).

2 **Impact**
To have a meaningful impact, the NCSC needed to be able to promote a technique across different media, in a way that could be quickly understood in most contexts. 'Three random words' contains all the essential information in the title, and can be quickly explained, even to those who don't consider themselves computer experts.

3 **Novelty**

The stereotypical password is a single dictionary word or name, with predictable character replacements. By recommending multiple words we immediately challenge that perception, and encourage a range of passwords that have not previously been considered.

4 **Usability**
The main issue with enforcing complexity requirements is that it's difficult for users to *generate*, *remember*, and *enter* complex passwords correctly without substantial effort, which further encourages the re-use of passwords. Three random words' power is in its usability, because security that's **not** usable doesn't work.

Responding to concerns

We do appreciate that some system owners may have concerns using the three random words technique over others. It may not be necessary across *all* organisations. For example, some will already be using good strategies for creating strong, unique passwords, and others will be uncomfortable moving to a model that's so different from what they currently use.

However, if you're not using 'three random words' for any of the following reasons, then you may want to consider adopting it.

1. 'There are search algorithms optimised for three random words'

This is true, but there are also search algorithms optimised for 'complex' passwords generated by humans (by far the most common type in use today). There have been many attempts to show which of these algorithms would be fastest at discovering human-generated complex passwords or three random word passwords, with the 'winner' depending on the assumptions made about people's behaviour. But it ultimately doesn't matter.

To be able to get an advantage from any optimised algorithm, you need to know which algorithm to use. So, given a large database where everyone is using different ways to generate their passwords, the effectiveness of any optimised algorithm is reduced. In the real world, this means the attacker must try several algorithms, which is harder (and takes longer) than trying just one.

Some people compare 'three random words' passwords with the 'random passwords created by password managers'. The latter are stronger than either 'three random words' or 'human-generated complex passwords'. However, this is not currently a useful comparison to make, as *there is still a very low uptake of password managers*. We hope more people will adopt password managers and this will also increase the diversity of passwords.

2. 'Three random words will generate 'weak' passwords, such as those that appear in common password lists'

There are many common passwords that conform to complexity requirements. For example, 'Pa55word!' may follow the complexity requirements for a website or service, but is a lousy password as it's quite guessable. Similarly, there are unique complex passwords (generated using three random words) that would not be permitted. Complexity requirements alone is a blunt instrument; to provide a more **targeted** removal of weak passwords, the NCSC recommend a minimum length requirement combined with the application of password deny lists.

3. 'People will struggle to remember passwords made from three random words for multiple accounts'

As we've discussed, to create passwords that meet complexity requirements we use coping mechanisms (which are well known to cyber criminals). Adopting three random words is **not** a panacea that solves the issue of remembering a lot of passwords in a single stroke, and we expect it to be used **alongside** secure storage.

Towards 'password diversity'

To make it harder for attackers, we need to increase the **diversity** of password use. This means reducing the number of passwords that are discoverable by cheap and efficient search algorithms, forcing an attacker to run multiple search algorithms (or use inefficient algorithms) to recover a useful number of passwords.

Currently, complexity requirements are actively working *against* password diversity (for all the reasons mentioned above). This has led to *convergence* in strategies and a reduction in password diversity. To increase diversity, we need to encourage people to use other password construction strategies (such as 'three random words'), that use length rather than character sets to achieve the desired strength. This effectively encourages the adoption of passwords that are currently unused, increasing password diversity in the ecosystem.

In the meantime, we hope that wider efforts across the technology sector to reduce our long-term reliance on passwords will bear fruit before convergence becomes a problem for three random words.

Kate R
People Team Lead, Sociotechnical Security Group, NCSC

* While there is a small risk of passwords being discovered in the storage location, this is outweighed by the benefits of users being able to use unique and strong passwords across their important accounts.

WRITTEN BY

Kate R
Sociotechnical Lead

PUBLISHED

6 August 2021

WRITTEN FOR

Large organisations

Cyber security professionals

Public sector

PART OF BLOG

NCSC publications

Inside the NCSC