NCSC lifts lid on three random words password logic

The logic of using three random words for strong passwords and why the NCSC advises the approach.

- National Cyber Security Centre (NCSC) explains the logic behind its long-standing password advice for the first time
- Using three random words is more secure than traditional advice built around 'password complexity', experts argue
- Approach allows creation of passwords to 'keep the bad guys out' whilst remaining easy to remember

Cyber security experts have today (Friday) revealed in depth for the first time the logic behind their advice to use three random words when creating passwords.

In a new blog post, experts at the National Cyber Security Centre (NCSC) – which is a part of GCHQ – said a key reason for using three random words is they create a password which is easy to remember and strong enough to keep online accounts secure from cyber criminals.

The blog post noted that using three random words to coin a password is more effective than traditional advice to create complex passwords, which can be difficult to remember and yet guessable for criminals.

Other reasons for choosing the three random words approach were:

- **Length**. Passwords made from multiple words will generally be longer than passwords made from a single word and therefore meet minimum length requirements.
- **Impact**. '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.

- **Novelty**. A password containing multiple words encourages a range of passwords that have not previously been considered.
- **Usability**. It's easier for users to enter a three random word password than one which contains a complex range of characters.

NCSC Technical Director Dr Ian Levy, said:

> "Traditional password advice telling us to remember multiple complex passwords is simply daft.
>
> "There are several good reasons why we decided on the three random words approach – not least because they create passwords which are both strong and easier to remember.
>
> "By following this advice, people will be much less vulnerable to cyber criminals, and I'd encourage people to think about the passwords they use on their important accounts, and consider a password manager."

Rocio Concha, Which? Director of Policy and Advocacy, said:

> "Ensuring you use strong yet memorable passwords online and with smart products is more important than ever – our research has repeatedly highlighted poor security practices in a range of connected devices, from routers and wireless cameras to apps.
>
> "There's a reason why new legislation announced by the government to improve standards for smart devices includes a ban on generic default passwords – these can make it easy for hackers to take control of devices or even your home network.
>
> "Strong passwords can stop cyber criminals in their tracks, and we'd urge everyone to ensure they adopt good practice to safeguard their data and privacy."

Creating passwords using three random words is one of the six key steps recommended by the cross government Cyber Aware campaign to protect accounts and devices from most cyber crime. More information can be found at cyberaware.gov.uk.

PUBLISHED

6 August 2021

WRITTEN FOR

Self employed & sole traders

Small & medium sized organisations

Large organisations

Public sector

Cyber security professionals

You & your family

NEWS TYPE

General news