Article

Mar 2023

Three small words...

When it comes to creating a new password for any service or system – whether in your professional or personal life - complexity requirements are becoming increasingly more demanding.

Alex Dicker
Security Consultant

Email alex.dicker@waterstons.com

This is to meet the increased capability of hackers and the ever-growing list of regulatory standards that are in place to keep our information secure.

A good password policy will ask you to consider a number of things, with the ultimate goal being to create a password that's complex enough to hold off a hacker.

For users, that doesn't make things easier - as humans the more complex something is the harder it is for us to remember.

Everyone has their own approach to creating passwords; maybe you swap an "O" for a "0" or an "I" for "1", but that doesn't necessarily make it any harder for a hacker to crack. In fact, you can find out if your account has already been hacked and your password revealed on Have I Been Pwned. This handy tool contains wealth of data compiled from dark web researchers. If you see your password on there, change it immediately.

Strong password policies will ask for a password that is:

- at least 12 characters long
- a combination of uppercase letters, lowercase letters, numbers, symbols
- and is totally different to any other password you've used before.

A quick and easy method for meeting these criteria, and creating a totally unique password each time, is to use the Three Random Words rule (passphrase) with a number and a symbol thrown in.

You can see in the below table how moving away from difficult to remember strings of digits and letters can make a password stronger an easier to remember:

Password	Time to crack
!@#$%^&*	2 Seconds
Z3nt!4$$	6 hours
grinningskydivingotter	3 years
GrinningSkydivingOtter	24 years
GrinningSkydivingOtter£33	20,000,000 years

This may not be the best method for you, but who could forget a grinning sky diving otter in a hurry?

You might find that your company already enforces a complex password policy, but this is also something you should be doing in your personal life.

How secure do you think your personal passwords are? Check out the top 200 most common and easy to crack passwords of 2022 to see if yours is on the list.

Moving away from passwords and creating easy to remember passphrases using methods such as three-random-words is in line with the advice currently given by the National Cyber Security Centre and its implementation can help your organisation align with access control requirements laid out in best practice standards such as ISO27001 or Cyber Essentials.

If you still think you'll struggle to remember three random words, consider using a reputable password manager. Just remember to use a secure password or passphrase that you can actually remember when you set up an account...

To find out more about how you can use our cyber security services to protect your team and your business, check out our page here.