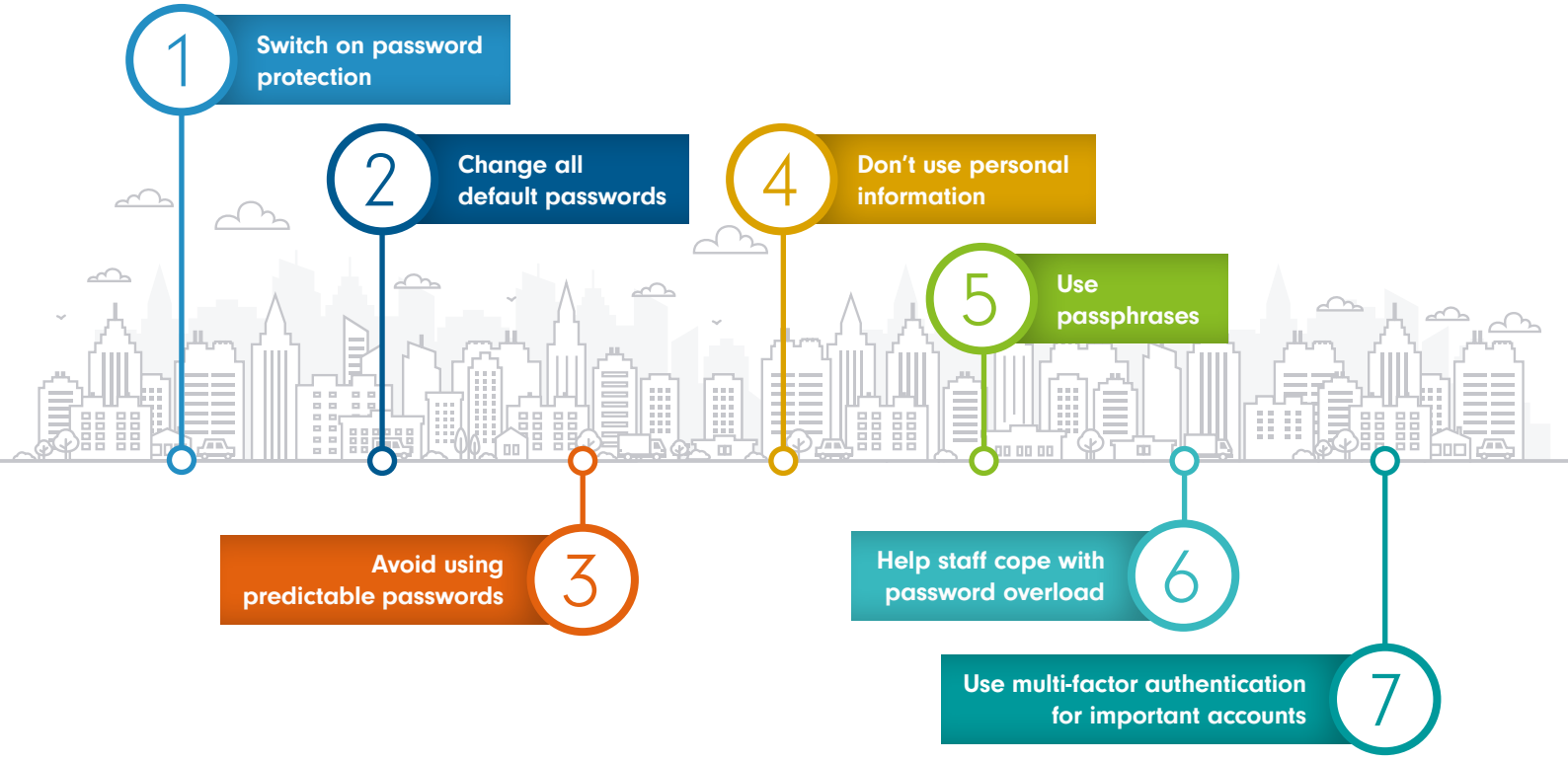
Do your passwords pass the password test?

In a world where cyber crime is an increasingly serious issue, safeguarding the systems and devices your business uses – such as computers, laptops, tablets and smartphones – is of the utmost importance. Any unauthorised access puts business-critical data, the personal information of your customers and also details of the online accounts that you access, at risk.

Passwords are an obvious way to prevent unauthorised access, although they need to be strong, robust and unique to be effective. However strong your passphrases or passwords are, there is always a chance that they could be hacked or stolen, through no fault of your own, so it's worth setting up an additional layer of security, in the form of multi-factor authentication.

Worryingly though, only 55% of individuals surveyed in the National Cyber Security Centre (NCSC) UK Cyber Survey admitted always using a strong password for their main email account. This is despite email passwords being particularly important, given these accounts commonly have a role in setting up and changing security details on other personal accounts.

In order to encourage password best practice within advice firms, we've highlighted some tips, largely based on advice from the NCSC.



FundsNetwork

Fidelity INTERNATIONAL

1 Switch on password protection

This can be as simple as setting up a screen-lock password or PIN. If you have a TPM (Trusted Platform Module) compatible device, you may also be able to enable strong biometric controls. This includes fingerprint or facial recognition, making it harder for hackers to gain access to your information as well as reduce the number of times you need to enter your password.

2 Change all default passwords

A very common mistake is not changing the default passwords that manufacturers issue with their smartphones, laptops, and other types of equipment. It's recommended that you change all default passwords before devices are given to staff. You should also regularly check devices (and software) to ensure that no default passwords are being used.

3 Avoid using predictable passwords

Using commonly-used and easy-to-guess passwords can be tantamount to opening the door to criminals. Indeed, breach analysis found that 23.2 million victim accounts worldwide used '123456' as the password. Other frequently-used passwords found in breaches included 'liverpool', 'chelsea', 'iloveyou' and everyday first names such as 'ashley' and 'michael' (with or without numbers added to the end).[1]

Passwords clearly need to be easy to remember but, on the other hand, they should be hard for somebody else to guess. A good rule to follow is to make sure that somebody who knows you well couldn't guess your password in 20 attempts. Within the workplace, IT systems should not require staff to share accounts or passwords in order to get their job done.

1. Source: National Cyber Security Centre/Troy Hunt.

4 Don't use personal information

As well as avoiding first names, staff should also steer clear of dates of birth, pet names and company names (e.g. 'fidelity123'). Indeed, any information that can be found on social media sites or online shouldn't feature as part of a password or as answers to the security questions needed to reset a password. They should be complex, obscure and difficult to guess.

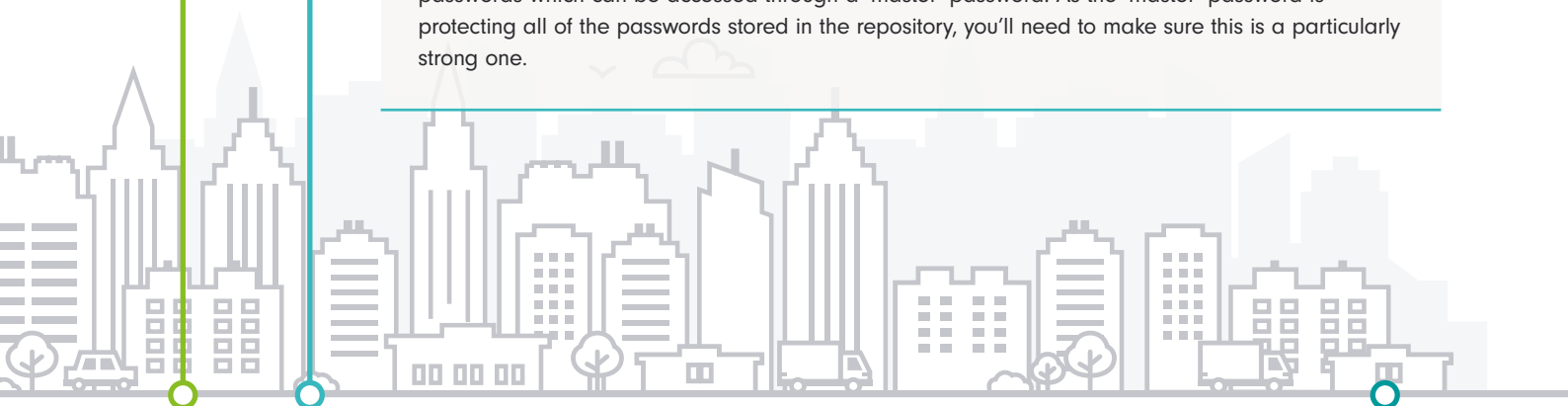
5 Use passphrases

Three randomly selected words in combination are stronger together as a 'passphrase' than typical passwords. Passphrases are more secure, simple to make and easy to remember. Predictable phases though, such as 'onetwothree', should be avoided.

6 Help staff cope with password overload

These days, most people tend to have around 200 online accounts and so remembering security details is a challenge. Therefore, within the workplace, it's a good idea to only enforce password access to a service if you really need to. Where passwords are used, the NCSC recommend that you don't require staff to regularly change passwords. Passwords really only need to be changed when you suspect a compromise of the login credentials.

You should also consider providing staff with a place to securely store passwords for important accounts. Using a password manager is an option – these are tools that can create and store passwords which can be accessed through a 'master' password. As the 'master' password is protecting all of the passwords stored in the repository, you'll need to make sure this is a particularly strong one.



7 Use multi-factor authentication for important accounts

You should use multi-factor authentication, if possible, for particularly important accounts – this significantly boosts security for not much extra effort. Also known as two-factor authentication or '2FA', it requires two or multiple different methods to 'prove' your identity before you can use a service. This is generally a password plus one other method, such as a code that's sent to your smartphone that must be entered in addition to the password.

Another crucial point on security...

As well as adopting a strong password protocol within your business, it's also strongly recommended that you ensure that every staff member has personal access to the right systems. Granting staff unnecessary system privileges or superfluous data access rights can be just as problematic as not allowing enough access. All users should be provided with a reasonable (but minimal) level of system privileges and rights needed for their role. These rights should be monitored and reviewed regularly, especially when a user is moving role or leaving the company.

For more information on how to proctect your business, visit our 'Technical resource centre' at fundsnetwork.co.uk and select 'Keeping your business safe'.

How we protect you and your clients

We understand the importance of keeping your firm's and your clients' information safe and secure. We use proven, industry-recognised security tools and processes to protect against fraud and security breaches and we regularly upgrade this protection in response to advances in security threats.

Fidelity is a member of Cifas, the UK's fraud prevention agency, which works closely with law enforcement partners. Cifas Protective Registration is a fraud protection scheme that helps us protect your clients should they be at risk of fraud.

If you have any concerns about security, please call us as soon as possible on 0800 358 7717.

More advice from the National Cyber Security Centre can be found on ncsc.gov.uk

FundsNetwork

Fidelity™ INTERNATIONAL

UKM1019/24914/SSO/1020