Do your passwords pass the password test?

In a world where cybercrime 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 online accounts you access, at risk.

Security measures like multi-factor authentication and biometrics are becoming increasingly common, however passwords will continue to play a role for the foreseeable future as they remain a fundamental layer of account security. They are an obvious way to prevent unauthorised access, although they need to be long, 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. It's therefore worth setting up an additional layer of security in the form of multi-factor authentication wherever possible.

In order to encourage password best practice within advice firms, we've highlighted some tips below, largely based on advice from the National Cyber Security Centre (NCSC).

Adviser Solutions

Fidelity INTERNATIONAL

1 Switch on password protection

This can be as simple as setting up a screen-lock password or PIN and also covers enabling multi-factor authentication and biometric controls. This includes fingerprint or facial recognition, making it harder for hackers to gain access to your information as well as reducing 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 and PINs that manufacturers issue with their smartphones, laptops, and other types of equipment including your home router. It's recommended that you change all default passwords and passcodes before devices are given to staff. You should also regularly check devices (and software) to ensure that no default login details are being used. With many organisations operating a mix of home and office work, it's especially important that default passwords are updated on home routers too.

3 Use long unique passwords

Using commonly-used and easy-to-guess passwords can be tantamount to opening the door to criminals. Indeed, breach analysis found that 7.6 million victim accounts worldwide used '123456' as the password. Other frequently-used passwords found in breaches included 'password', 'abcd1234', and 'qwerty123'.[1]

Passwords clearly need to be easy to remember but, on the other hand, they should be hard for somebody else to guess. The National Cyber Security Centre (NCSC) recommends combining three random words to create a single password that is long and strong. Within the workplace, IT systems should not require staff to share accounts or passwords in order to get their job done.

1. Source: cybernews.com.

4 Don't use personal information

As well as avoiding first names, staff should also steer clear of dates of birth, favourite sports team names, pet names, 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. Sites like LinkedIn and Facebook are one of the first places a hacker will visit to build up a profile of you.

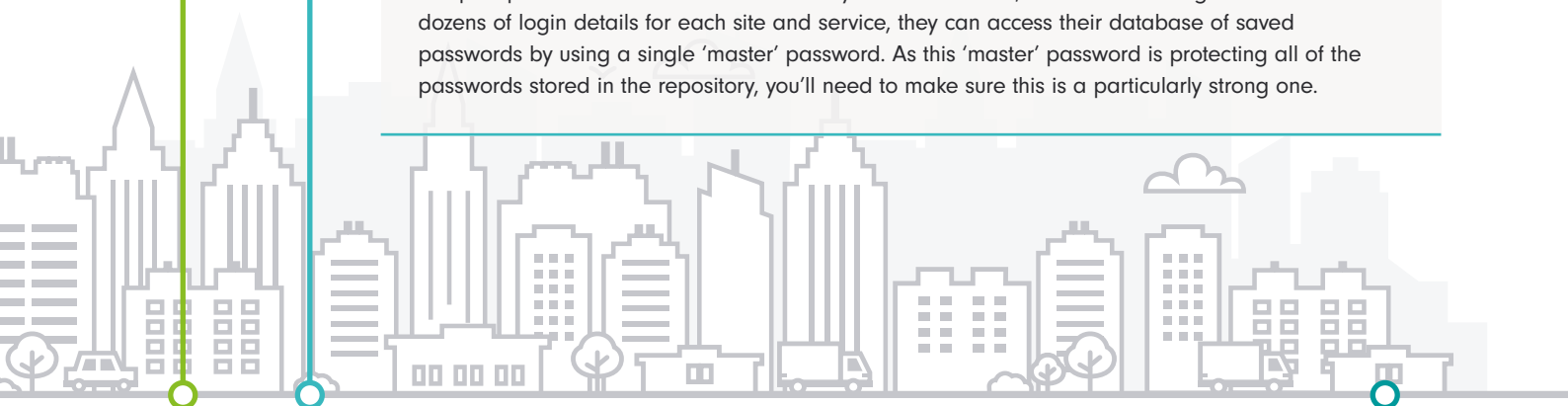
5 Use passphrases

Three randomly selected words in combination are stronger together as a 'passphrase' than typical passwords. Passphrases are longer, more secure, simple to make and easy to remember. Predictable phrases though, such as 'onetwothree', should be avoided. A good approach is to take three or more completely unrelated words and sprinkle them with a mix of upper- and lower-case characters, numbers and special symbols.

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. The NCSC recommends 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 long, highly complex passwords and store them securely. This means that, rather than having to remember dozens of login details for each site and service, they can access their database of saved passwords by using a single 'master' password. As this '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 wherever possible but especially for important accounts like your primary email account – this significantly boosts security. Also known as two-factor authentication or '2FA', it requires two or more pieces of information (like a password and a one-time code sent by SMS) to 'prove' your identity before you can successfully enter the account. If a company, application, website or service offers multi-factor authentication you should definitely use it.

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 the minimum amount of administration rights and access privileges they need to perform their role, and no more. 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 protect your business, visit our Technical matters hub

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

Adviser Solutions

Fidelity INTERNATIONAL

UKM1225/LM/QC/1126

[WF-3433835]