Your guide to

Passwords

An information security eBook by TSC

Inspire. Engage. Protect.

Passwords: important, but often overlooked

We all know how vital it is to have a strong password – you will have heard the message repeatedly, from your workplace password policy to the increasingly complicated password requirements of your online accounts.

Despite this, cybersecurity incidents continue to increase year-on-year.

FACT

81% of confirmed data breaches in 2017 involved weak, default or stolen passwords[1].

So, if we recognise the importance of strong passwords, how are cybercriminals still able to commit successful attacks?

The truth is that our password behaviour still leaves a lot to be desired. SplashData analysed 5 million exposed passwords from 2018, and the results proved that many of us are still using weak, easily cracked passwords.

Many of us also engage in other poor password practices. Saving passwords in browsers, sharing passwords with others and reusing passwords across different accounts are just some of the ways we are putting our security at risk.

Read on to find out why we need to improve our password behaviour, and what we can do to stay safe in the face of cybersecurity threats.

[1] Verizon Data Breach Investigations Report, 2017

Weakest passwords of 2018[2]

A CLOSER LOOK

A 2018 report from Dashlane revealed that even celebrities and government officials aren't immune to choosing terrible passwords.

At the top of Dashlane's list of 'Worst Password Offenders' was American rapper Kanye West, who revealed during a televised meeting with Donald Trump that his **iPhone passcode** was '**000000**'.

The Pentagon came a close second. When the Government Accountability Office (GAO) carried out a cybersecurity audit, they were able to guess admin passwords in only **nine seconds**.

They also found weapons systems software was protected by **default passwords** that anybody could find online.

[2] SplashData, Worst Passwords of the Year, 2018

How are passwords cracked?

To understand how to protect ourselves from criminals who want to steal our passwords, we first need to understand **how** they do it.

When we hear about accounts being 'hacked' and passwords being 'cracked', it often conjures an image of a tech-savvy teenager in a hoodie. The adolescent hacker is usually sitting in a dark room, surrounded by program code, and typing furiously at his computer.

However, this image is false – almost anybody can pinch your passwords with very little, if any, technical expertise. Password cracking software, for example, is commercially available and can be used to quickly guess and test thousands, or even millions, of passwords every second.

Let's take a look at some of the most common ways passwords are cracked or stolen.

Brute force attack

Fast-paced trial and error

A brute force attack involves a cybercriminal systematically working through all possible combinations of letters, numbers and special characters until they find your password.

This is generally carried out using computer software which can run through thousands of guesses in a matter of seconds.

It can be a fairly quick process for short passwords, but longer passwords take much longer to crack because they have many more possible characters that need to be checked.

For example, if you had a password that contained 8 characters, including letters and numbers, then a brute force attacker would have to work through **200,000,000,000,000 possibilities**. But if you increase it to 12 characters then this would increase to **100,000,000,000,000,000,000,000 possibilities**.

This is why you're always being pestered to make your password as long as possible.

More attack methods

Dictionary attack

Brute force, with a book

A dictionary attack is a type of brute force attack which is used for longer passwords where a basic brute force attack would take too long.

Using this method, a cybercriminal will try to determine your password by checking thousands of possible words from dictionaries and lists of previously breached passwords.

The cybercriminal will also **check for common substitutions, such as '1' for 'i' or '@' for 'a'**. So, replacing a few letters in your password with numbers or symbols won't protect you from this type of attack.

Using the dictionary attack method, a password like P@ssw0rd, if it didn't already appear on a breached password list, would be cracked in about 9 hours[3].

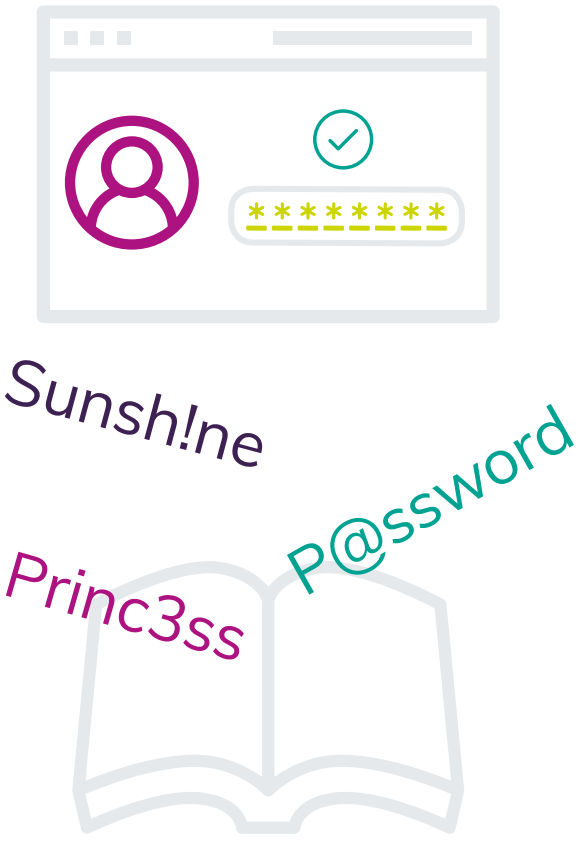
FACT

At the time this eBook was published, P@ssw0rd had appeared in data breaches 52,579 times[4].

DID YOU KNOW?

Cybercriminals using brute force or dictionary attacks will keep guessing at your password until they find the correct one, but you get locked out of your account after three incorrect guesses – so you're safe, right?

Actually, most of these attacks take place offline using a stolen password file, which means a cybercriminal won't try your password online until they know it's correct.



[3] Dashlane, How Secure is my Password?
[4] Have I Been Pwned, Pwned Passwords

Phishing for passwords

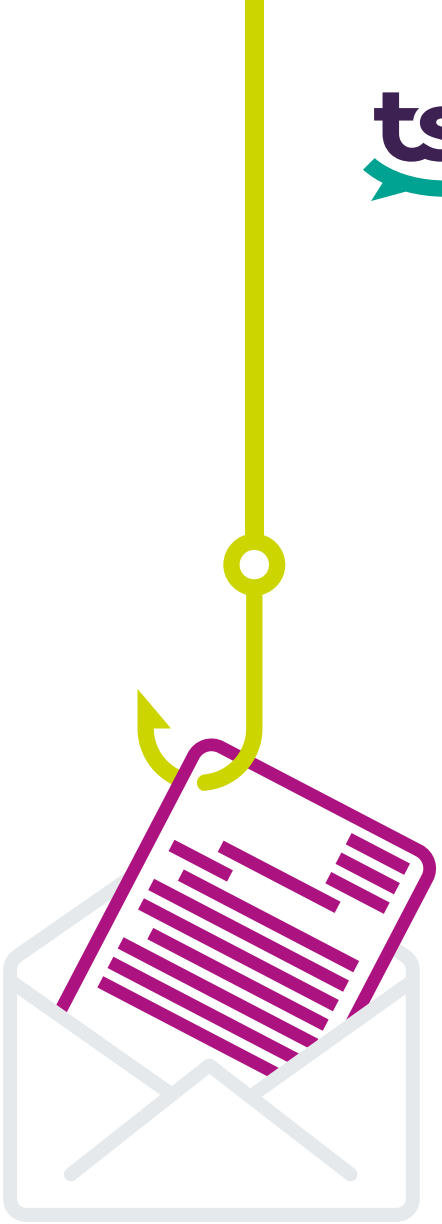
Social engineering

Tricking you into giving it away

Phishing is popular with cybercriminals because it's an inexpensive way of reaching thousands of potential victims, meaning it's profitable even if only a few people fall for it.

While you may think you'd never be deceived by a phishing attack, the truth is that they are becoming increasingly sophisticated and difficult to detect. Cybercriminals use various methods to try to steal your data and may use multiple points of attack within the same phishing campaign[5].

As well as phishing, cybercriminals have other tricks up their sleeves to dupe you into revealing your password. For example, they may call you pretending to be somebody you know and trust, such as your IT department, and ask for your password. Or they could simply watch over your shoulder as you type it into your computer or device.



FROM THE ARCHIVE
March 2019

PHISHING ATTACK MIMICS iOS BROWSER BEHAVIOUR[6]

A phishing campaign that targets iOS users could be adapted 'very easily' for Android devices, researchers have warned.

Researchers at Myki, a password managing software company, reported that the campaign leads victims to a malicious page to trick them into entering their social media credentials.

The attack begins with a fake Airbnb website which prompts the user to log in via Facebook.

When the user clicks to log in, the page automatically shows a video of browser tabs switching so that it appears genuine.

Antoine Vincent Jebara, CEO of Myki, said:

> "From the moment a user accesses the malicious website, they are manipulated into performing actions that seem legitimate, all with the purpose of building up their confidence to submit their Facebook password at the final stage of the attack."

[5] Microsoft Security Intelligence Report Volume 24, 2019
[6] Myki, Mimicking Native iOS Behavior in Facebook Phishing Campaign, March 2019

Other ways to crack your password

Malware

Stealing it from beneath your fingertips

Cybercriminals may use malicious software (malware) to steal your passwords directly from your device. This type of attack often starts with a phishing email which encourages you to open an attachment or click a link. This triggers the download of malware, which will infect your device and possibly your entire network.

One common type of password-stealing malware is a keylogger. This software records the keys you hit on your keyboard to collect your usernames, passwords and even financial information.

Similarly, a screen scraper takes screenshots of your device as you type your password and sends the images back to the cybercriminal.

Open source intelligence (OSINT)

Scouring your social media

Using public sources, such as your social media accounts, cybercriminals can gather a wealth of information that will help them guess your passwords.

Think about the information you post online, such as the names of your pets or the town you grew up in. Perhaps they'll be able to work out the date of your anniversary or a friend's date of birth based on photos from special occasions.

Personal information like this is commonly used in passwords and as answers to security questions. All a cybercriminal has to do is enter the key words or dates they have found into their password-cracking software and it will work through thousands of possible combinations until they find your password.

A CLOSER LOOK

The number of people targeted by password-stealing malware, also known as password stealing ware (PSW), increased by 60% in just one year.

Researchers from Kaspersky found that the number of people targeted rose from 600,000 in the first six months of 2018 to more than 940,000 in the first six months of 2019[7].

[7] TechRadar, Major rise in password-stealing malware detected, July 2019

How can I protect myself?

Now that we know how cybercriminals might attack us, let's take a closer look at how you can improve your password behaviour to help protect yourself from their attacks.

Create strong passwords

Weak and commonly used passwords put your accounts at significant risk of being compromised using brute force or dictionary attacks. You therefore need to create passwords that are strong enough to withstand these attacks.

Unfortunately, there is a lot of different, and sometimes contradictory, information available about what constitutes a strong password.

To help you cut through the noise, here are some top tips you should follow:

Longer is stronger

The more characters you use in your password, the longer it takes to crack in a brute force attack. For example, a password containing 5 characters would take 10 seconds to crack, whereas a password with 8 characters could take 155 days to crack. Increase it to 10 characters, and the software would struggle to crack it within 3000 years[8].

Discard the dictionary

Never use single dictionary words or very simple passwords such as '123456'. These words will be cracked extremely quickly by a cybercriminal using the dictionary attack method.

Refrain from using personal information, such as your pet's name or the dates of special occasions, as these can be easily discovered by cybercriminals using social engineering or by researching your online profiles.

FACT

The password '123456' has been seen over 23.5 million times in data breaches[9].

[8] InfoSec Institute, How easy is it for a hacker to crack your password?, February 2017
[9] Have I Been Pwned, Pwned Passwords

Make life easier with a passphrase

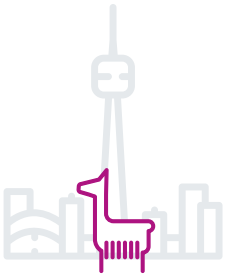
Pick a passphrase

Creating a long, strong, memorable password can be difficult, so try creating a passphrase instead.

Your passphrase should contain three unrelated words that you can remember, such as a colour, animal and destination.

For example:

PurpleLlamaToronto



Using a phrase instead of one word can help defeat dictionary attacks. It also helps you to easily create a longer password – this 19 character passphrase would take a computer about 6 trillion years to crack.

You can go one step further to make your password even more secure by replacing some of the letters with numbers or special characters.

For example:

Pu7pleLlam8Toron£o

This password would take 7 quadrillion years for a computer to crack.

Make sure it hasn't been compromised

Once you've created your password, it's a good idea to check it against lists of commonly used and previously breached passwords.

This is because once a password has been compromised, cybercriminals will use a method known as password spraying to try that password for lots of different accounts.

If you're not sure where to find a list of common or breached passwords, **Have I Been Pwned** is a great place to start.

DID YOU KNOW?

It is a common misconception that you must use numbers and special characters to create a strong password. The length of your password is actually much more important than its complexity.

In fact, forcing restrictions such as the use of special characters often encourages people to create weak passwords and simply tweak characters until it meets the requirements.

So, if you think you'll be able to remember it then feel free to add special characters to your password. But, if not, just make sure it's long and strong.

What else can I do?

Make your passwords unique

You might think a breach of, for example, your Twitter password, is not a big deal – you don't store any financial data in your account and it only contains basic personal details.

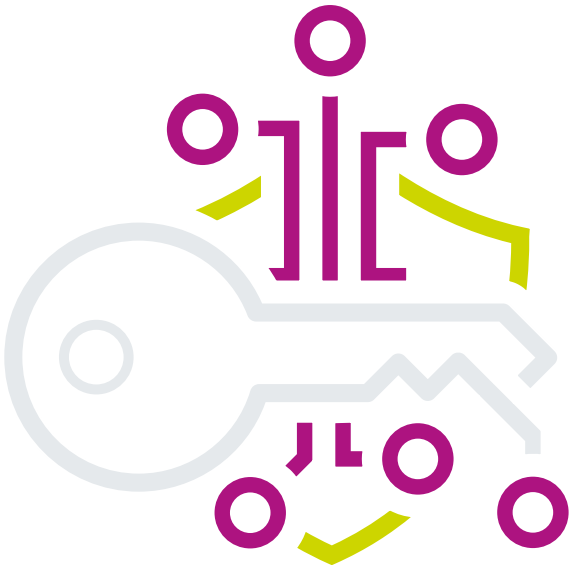
However, evidence suggests that many of us reuse our passwords across various accounts. Once one password has been compromised, cybercriminals will attempt to use it for all of your accounts – this is called credential stuffing. They can do this incredibly quickly using easily available software.

This puts you at an increased risk of fraud and identity theft.

The average person owns 200 password-protected accounts[10]. So, the problem with creating a different password for each account is that it's impossible to remember that many passwords. Follow our top tips to create, and keep track of, unique passwords.

FACT

51% of people reuse an average of 5 passwords across business and personal accounts[11].



Use a password manager

A password manager is the secure equivalent of writing your passwords down or storing them in your browser. It stores all your passwords and automatically populates the password field when you want to log into saved websites. Many password managers also allow you to save notes, such as answers to security questions or PIN codes for offline accounts, meaning everything is in one secure location.

Your password manager can also generate strong passwords and save them straight to your account, so you don't have to think of or remember them yourself.

If you're considering using a password manager, always do your research first to make sure it's reputable. You will also need to create a very strong master password for your account.

FACT

42% of people save passwords in their browser[12].

[10] Dashlane, Kanye West Tops Dashlane's list of 2018's 'Worst Password Offenders', December 2018
[11] Ponemon Institute, The 2019 State of Password and Authentication Security Behaviours Report
[12] NCSC, UK Cyber Survey, 2019

Alternatives to passwords

Think about other options

These days, there are lots of different methods available for securing your computers, devices and accounts.

Many computers and devices, for example, now allow you to log in using biometric identifiers, such as your fingerprints. Or you could use a hardware token, such as a USB key, to authenticate yourself when logging in.

However, even with these other options, you often need a password or passcode as a backup, so make sure it's long and strong. Save it in your password manager, if you have one.

FACT

57% of people prefer using passwordless logins[13].

[13] Ponemon Institute, The 2019 State of Password and Authentication Security Behaviours Report

Don't give it away

Keep your passwords secret

Of course, there's no point creating a strong, unique password and locking it in a password manager if somebody else knows it. Whether that's a cybercriminal or a friend.

It's essential that you keep your password to yourself – do not reveal it to anybody, even to family or friends. The fewer people who know it, the fewer points of attack for a cybercriminal.

If you have a shared account, meaning that the password must be shared with somebody else, make sure you share it securely via encrypted email or from within your password manager.

Stay safe from social engineers

Social engineers have lots of tricks up their sleeves to try to steal your password, from phishing emails and phone calls to fake websites. Take a look at the 'How are passwords cracked' section in this eBook to find out more.

Common signs of phishing emails include:

- Email addresses that don't match the sender
- Blanket or generic greetings such as 'Dear customer', 'Hi', or your email address
- Unusual attachments, links or buttons
- Urgent or unusual requests
- Spelling or grammar errors

FACT

69% of people admit sharing passwords with their colleagues[14].

Protect yourself from malware and phishing websites by never clicking on links or opening attachments in suspicious emails.

Also be alert to phishing attacks carried out over the telephone, known as **vishing**, or in a text message, known as **smishing**. Be particularly wary of:

- Unsolicited calls or texts
- Urgent or threatening language
- Offers or deals that seem too good to be true
- Suspicious numbers that don't look like real mobile phone numbers
- Shortened links that disguise the destination

Protect yourself by never providing personal or password information in response to an email, call or text message. If you think it might be genuine, call the person back on a known, trusted phone number.

You should also look out for shoulder surfers who may watch as you type in your password or PIN. Shield your information from prying eyes.

[14] Ponemon Institute, The 2019 State of Password and Authentication Security Behaviours Report

Staying safe online

Be social media savvy

You might be surprised by how much information about you is online, and how much of it could be used to compromise your passwords.

You may not have even shared the information consciously. For example, have you ever taken a fun social media quiz such as 'Discover your showbiz name'? Perhaps it told you to simply enter your pet's name and your mother's maiden name to reveal your showbiz moniker.

Always think carefully about posting personal information on the internet and social media.

Remember that what goes online, stays online.

Change default passwords

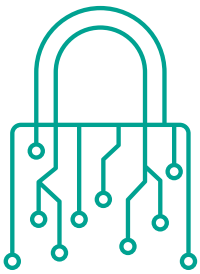
Nowadays, many of our devices, including everyday household appliances, are connected to the internet – this collection of connected devices is known as the Internet of Things (IoT).

While these devices have many benefits, don't forget that anything connected to the internet could be compromised.

You are much more likely to be successfully attacked if your device doesn't have a password or if it uses a default password. Default passwords can often be found with a quick online search.

Before you connect anything to the internet, password-protect it and always change default passwords.

If it has a connection, it needs protection.



Find out more

Interested in the security of IoT? Read our Internet of Things eBook, available now on our website.

The problem with default passwords

FROM THE ARCHIVE
September 2019

WEBCAMS CAN BE ACCESSED USING DEFAULT PASSWORDS[15]

A security researcher has discovered 15,000 IoT webcams that can be easily accessed by anybody with an internet connection.

The devices, made by multiple companies worldwide, are protected by default passwords that can be easily discovered or guessed by cybercriminals.

Chase Williams, Web Security Expert at WizCase, said:

> "Some examples of camera that were accessible include those at shops, inside kitchens/living rooms/offices of private family homes – including a live feed of people on the phone and children peeking at the camera directly, tennis courts, storage units, hotels, museum security feeds, churches, mosques, parking lots, gyms, and more."

[15] Teiss, Thousands of private webcams used worldwide lacking basic security protections, September 2019

Additional security measures

Use extra protection

No matter what we do, passwords remain a relatively weak method of authentication. However, it looks like they're here to stay for the foreseeable future.

You should use additional security measures wherever possible to support your passwords.

Use multi-factor authentication

One of the most effective options for additional protection is two-factor or multi-factor authentication (2FA/MFA). These require you to authenticate yourself using additional measures in conjunction with your password. For example, using biometrics, a USB key or a passcode sent to your phone or email address.

This means that even if somebody steals or cracks your password, they will be unable to log in to your account as they do not have the secondary identifier.

Update your systems and software

It is surprising how often people will update their anti-virus software and operating systems on their computers and laptops, but then completely forget about their mobile phones or tablets.

And it's not just these types of devices that need updating. You should keep all your connected devices, including your smart TV or even a smart fridge, updated.

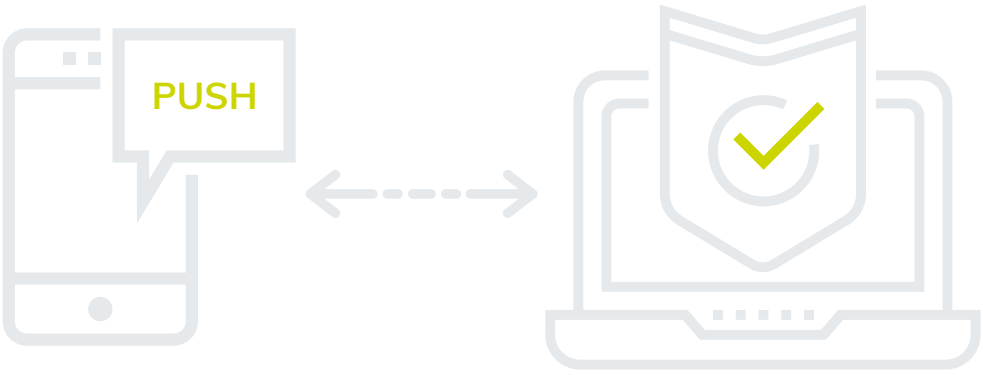
If you're unsure how to do it, take a look at the device manual or give the supplier a call.

FACT

Text message-based 2FA can block up to 100% of automated bot attacks, 96% of bulk phishing attacks, and 76% of targeted attacks[16].

FACT

38% of people do not run updates on their smartphones or tablets, while 55% of people do not run updates on their smart TVs[17].



[16] Google, New research: How effective is basic account hygiene at preventing hijacking, May 2019
[17] Bitdefender, The IOT Threat Landscape and Top Smart Home Vulnerabilities in 2018

Help!
I've been breached

No matter what we do, we can never be completely protected against a determined cybercriminal – so what can you do if the worst does happen and your password is stolen or cracked?

Firstly, make sure you're notified as soon as possible of breaches that could affect you.

Sign up for updates from the **Have I Been Pwned** website, which tells you when your email address appears in a known data breach.

Remember that companies are also required under the EU General Data Protection Regulation (GDPR) to inform customers if they are affected by a data breach.

You should also stay up to date with cybersecurity news.

If you realise that somebody knows your password or if you are notified of a breach affecting you, take it seriously.

DID YOU KNOW?

If your data or password has been breached, this is known in the tech-world as being '**pwned**' (pronounced 'owned').

The origins of the word 'pwned' are not entirely clear, but a popular theory is that when players of the online game 'World of Warcraft' lost a game, they were said to have been 'owned'. A map designer for the game, as the story goes, misspelled the word and so 'pwned' was born.

Limiting the impact of a breach

Follow these steps to protect yourself, your accounts and your information:

- Do not click on any emailed links to 'reset your password' as this could be a phishing attempt. Instead, log into the affected website directly and change your password from there.
- Immediately change your password and the passwords for any other accounts that use the same or similar passwords. Make all your passwords unique to each account.
- When resetting your password, never simply change one character or add another letter or number to the existing password. Cybercriminals will try all possible versions of your password.
- Log out of the account on all devices that you may be logged into it on. Some websites, such as Facebook and Google, allow you to log out of all web sessions remotely.
- Keep an eye on your accounts, including your bank account, and contact the organisation directly if you notice any suspicious activity.
- Keep your systems and anti-virus programmes up to date on all devices.
- If a work account has been compromised, immediately follow the appropriate procedures.

Conclusion

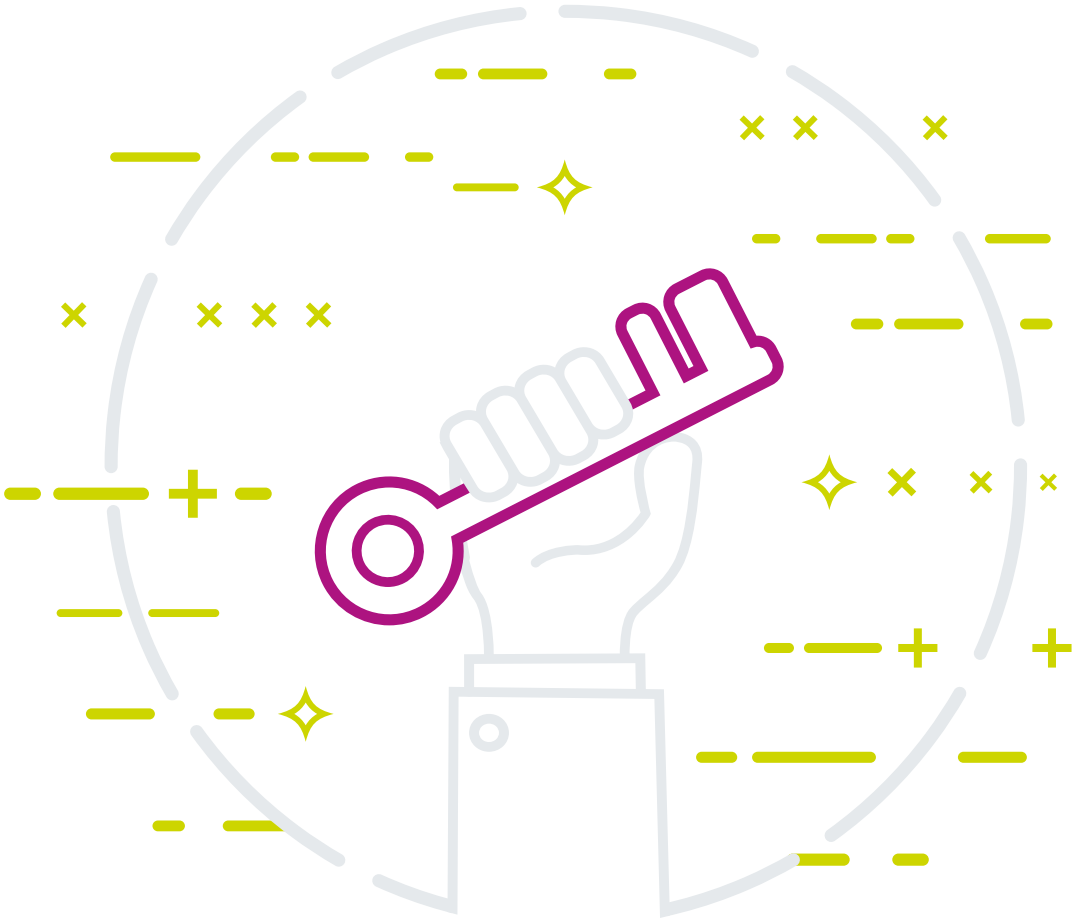
Passwords are vulnerable, but there are steps we can take to help protect ourselves.

As data breaches continue to increase, as technology evolves, and as cybercriminals create new methods to attack us, we can't ever be completely safe.

But we can't afford to be complacent with our passwords – we must stay up to date with the most recent advice and use extra protections such as 2FA or MFA whenever we can.

By following the practical advice we have given you in this eBook and in the following password checklist, you will be in a stronger position to protect yourself.

And if you found it useful, pass it on to your family, friends and colleagues, too. Together, we are safer.



Your password checklist

There was a lot of information in this eBook, and we want you to remember as much of it as possible.

Here is a summary of our top tips for you to print, cut out and keep. Place it somewhere prominent, and you'll be on your way to protecting your information with powerful passwords in no time.

Password power

Create strong passwords

- ◯ Make them as long as possible
- ◯ Do not use single dictionary words or words that are personal to you
- ◯ Use a passphrase containing three unrelated words
- ◯ Check breached password lists, such as Have I Been Pwned
- ◯ Consider passwordless logins

Keep your passwords secret

- ◯ Store passwords securely in a password manager
- ◯ Don't share passwords between accounts or with other people
- ◯ Watch out for phishing emails, calls and texts
- ◯ Think carefully before posting personal information online
- ◯ Change default passwords

Use extra protection

- ◯ Use multi-factor authentication where available
- ◯ Update your operating systems and anti-virus software on all devices

Help! I've been breached

- ◯ Do not click any emailed links to 'reset' your password
- ◯ Immediately change your password on all accounts using the same or similar passwords
- ◯ Change passwords completely – don't just add a new character
- ◯ Log out of the compromised account everywhere
- ◯ Look out for suspicious activity on your accounts

www.thesecuritycompany.com

Inspire. Engage. Protect.

Contact TSC for more information about perfecting and protecting your passwords and for other information security support and resources.

www.thesecuritycompany.com

@thesecuritycompany

@thesecurityco

@thesecurityco

Inspire. Engage. Protect.