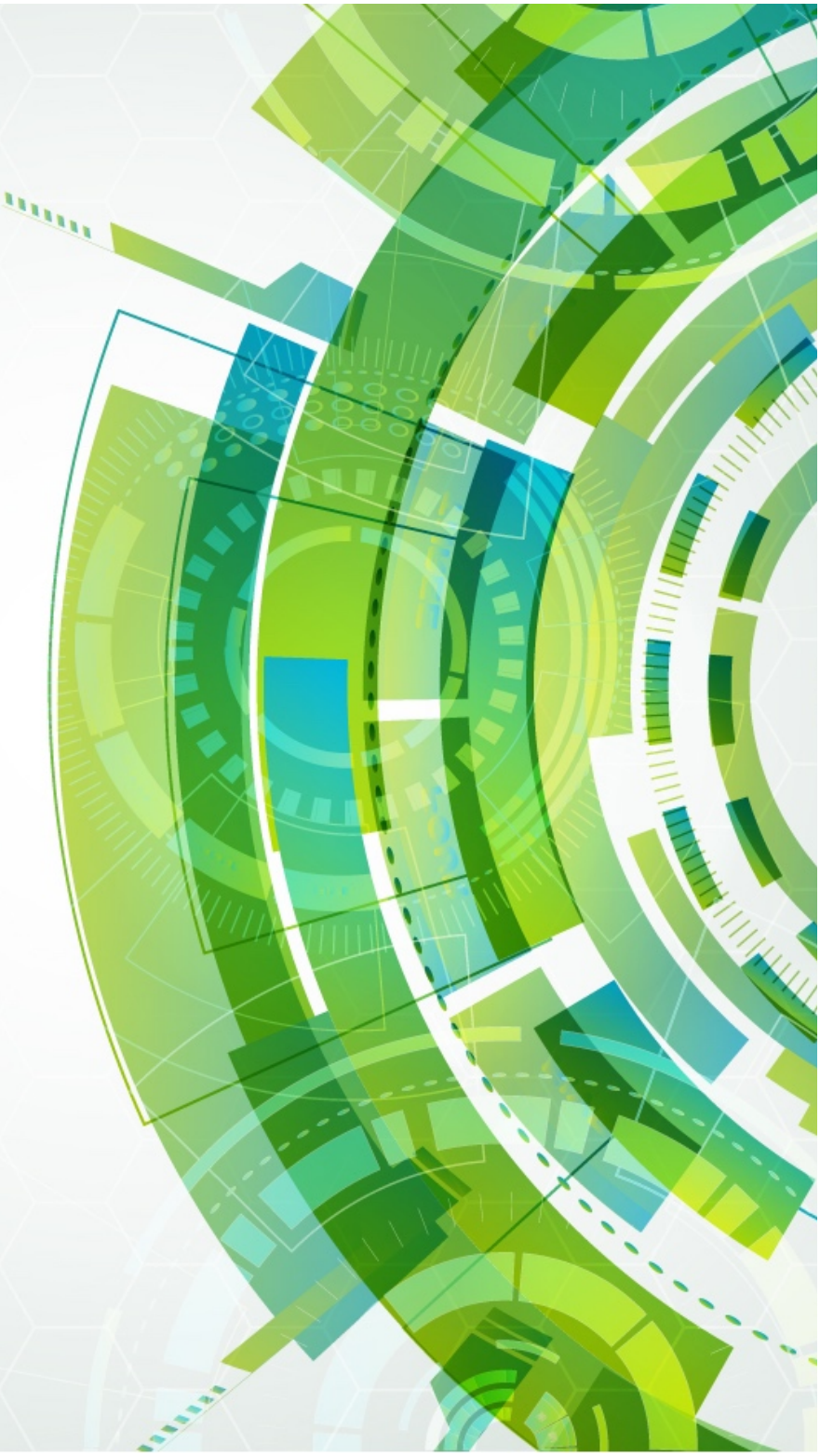
A NEW ERA FOR

Password Security

By Julia O'Toole



As our world becomes increasingly digitalised, our need for passwords rises. Not so long ago, we could rely on just a few passwords. Today, most internet users will have upwards of 100 passwords.

MYCENA
Protect Passwords

An increasingly digitalized world means password use will surpass 300 billion by 2020.[1]

As our world becomes increasingly digitalised our need for passwords rises. Not so long ago, we could rely on just a few passwords. Today, most internet users will have upwards of 100 passwords. And the problem is growing. A recent report states that password use is increasing rapidly and is likely to surpass 300 billion by 2020.[1]

This whitepaper explores the password security landscape, from people's understanding of password usage to introducing a new way to protect your passwords so they can protect you.

1 Cybersecurity Ventures
The World Will Need to Protect 300 Billion Passwords by 2020
https://www.inc.com/joseph-steinberg/300-billion-thats-how-many-passwords-may-be-in-use-by-2020.html

Why passwords exist in the first place

Passwords were devised to offer a simple way to prove your identity when using websites, email accounts and applications. A password is the digital equivalent of a key to give you access to your private online environments. It proves it's you and that you have the right to enter.

Passwords are the keys that open the front door to our digital world

Why we still use high-risk passwords

The challenge we now face is that we have too many passwords to remember. And when you try and keep too many number and phrase combinations in your mind, you start to mix them up.

The problem is the stronger the password, e.g. lots of letters (in upper and lower case), numbers and characters, the harder it is to remember. That's why we tend to default to simple combinations that are easy to recall.

The trinity of password sins

Users often think they have no choice but to revert to something they can control. We call the following the trinity of password sins

1. Using weak passwords
2. Reusing passwords or variations
3. Writing passwords down on post-its, in notebooks and Excel spreadsheets

Your passwords are vulnerable to credential stuffing, phishing, social engineering

Are you increasing your risk of attack?

If you're guilty of any or all of the above password sins, you put your whole business at increased risk of attack by cyber criminals, who will:

1. Use leaked usernames and passwords for credential stuffing and to access other accounts
2. Use phishing to lure people to give their credentials
3. Use social engineering to extract information for identity theft

Why passwords are now a huge threat to businesses

According to the Verizon Data Breach Investigations Report, over 80% of hacking-related breaches were linked to weak, reused or stolen passwords.[1] That's an alarmingly high figure.

Expanding beyond business systems and infrastructures, the surface of attack is now to the whole workforce. From chief executives to junior employees, anyone who is connected to the internet is vulnerable to cyber-attack and poses a potential risk.

But most UK adults are unsure how they should protect their passwords with the majority using the following unsafe methods: [2]

53% Human memory

32% Save in browser

26% Spreadsheets

26% Write it down

1% Other

Every business is at risk

According to a government report, 43% of businesses experienced a cyber security breach or attack in the last 12 months.[4] The average cost of breaches across all UK businesses amounted to an average of £3,100.[3]

Sensitive industries face biggest threat

The biggest threats are to those in sensitive areas such as defence, police, government, energy, water, utilities, infrastructure, technology, banking, healthcare, pharmaceuticals, transport, and law.

Through a ripple effect, whole communities and countries may suffer the impact of a breach.

Companies don't always realise there is a breach

Many businesses have failed to recognise a cyber security breach when it occurs, with 93% of data breaches going undiscovered for weeks.[1]

1 Verizon Data Breach Investigations Report https://www.verizondigitalmedia.com/blog/2017/07/2017-verizon-data-breach-investigations-report/

2 Verdict: https://www.verdict.co.uk/password-security-surveillance-fears/

3 Cyber Security Breaches Survey 2018 from the Department for Digital, Culture, Media and Sport https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/702074/Cyber_Security_Breaches_Survey_2018_-_Main_Report.pdf

During that time a huge amount of damage can be done. Hackers can install malware on an employee's computer that can extract sensitive information from your network before you even realise your security's been breached.

Password habits are getting worse

Despite the risks outlined, password habits are getting worse.

SplashData publishes an annual list of Worst Passwords of the Year [1] by evaluating more than 5 million passwords leaked on the internet. Its findings reveal that computer users are still using the same predictable, easily guessable passwords despite the significant risk of being hacked and having their identities stolen.

Here are the top ten worst passwords of 2018. SplashData estimates almost 10% of people have used at least one of the 25 worst passwords on this year's list – and nearly 3% have used the worst password, 123456.

1. 123456
2. password
3. 123456789
4. 12345678
5. 12345
6. 111111
7. 1234567
8. Sunshine
9. Qwerty
10. iloveyou

The risk of breach by password gets higher every year

2018 was the worst year so far for cyber security breaches. This was hotly followed by the two largest leaks of usernames and passwords in history, named Collection#1 [2] and Collections #2-5 [3] in January 2019.

As people need more account passwords, they increase their risk of getting hacked by reusing the same one.

Does your business take cyber security seriously?

Even though 74% of businesses and 53% of charities say that cyber security is a high priority for their organisation's senior management

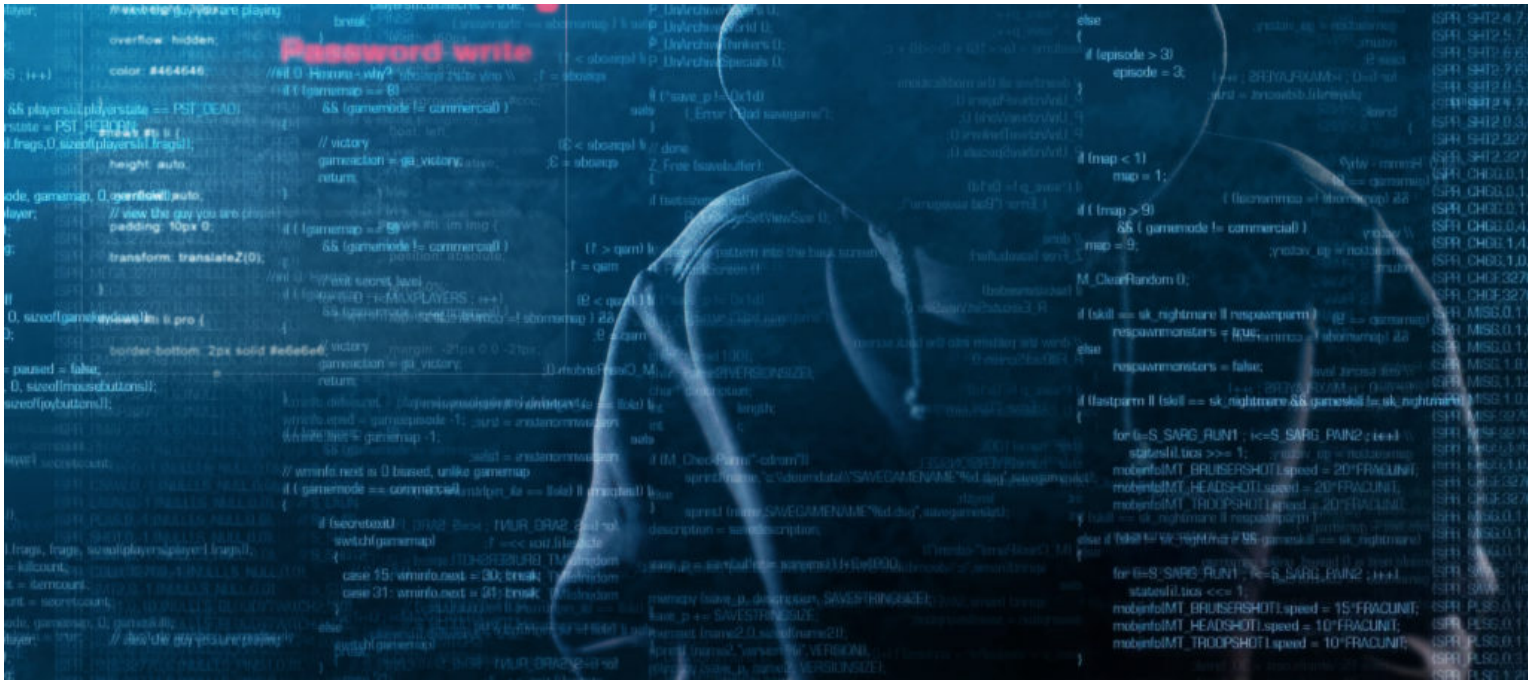
10% of people have used at least
one of the 25 worst passwords

Collections #2–5 represents 845 gigabytes
or 2.2 billion stolen credentials including usernames and passwords.

1 SplashData's Top 100 Worst Passwords of 2018
https://www.teamsid.com/splashdatas-top-100-worst-passwords-of-2018/

2 Forbes https://www.forbes.com/sites/kateoflahertyuk/2019/01/17/collection-1-breach-how-to-find-out-if-your-password-has-been-stolen/#3c2d829a2a2e

3 Wired https://www.wired.com/story/collection-leak-usernames-passwords-billions/



- Only 27% of businesses and 21% of charities have a formal cyber security policy or policies.[1]
- Only 9% of business have a cyber-security insurance policy in place.[1]
- Only 4% of charities have a cyber-security insurance policy in place.[1]

Do you know how hackers operate?

Okay, so your password's not exactly original, but what harm can it do? To answer that question, you need to know how a hacker thinks, to prevent yourself from being hacked.

You need to know how a hacker thinks to prevent yourself from being hacked

The brute force method

With the brute force method, hackers run scripts to test combinations and their variations onto multiple services to 'guess' your password by trial. It makes a high number of attempts per minute.

The software can be programmed to focus on words and numbers linked to you such as names of loved ones and birthdays. A quick browse of your online profiles on Facebook, Twitter and LinkedIn could soon reveal these.

Or, since there are billions of usernames and passwords available on the internet – there's a high chance yours is there too. Hackers can learn from those variations to 'guess' faster.

How often have you tried this method yourself when you've forgotten your password? You enter the password you think you used until you find the right one. Most passwords can be cracked within 24 hours using a brute force tool that can be downloaded for free.

1 Cyber Security Breaches Survey 2018 from the Department for Digital, Culture, Media and Sport https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/702074/Cyber_Security_Breaches_Survey_2018_-_Main_Report.pdf

Dictionary and spidering attacks

Another common hacking strategy is the dictionary method. This uses a simple file containing words that can be found in a dictionary.

An alternative is to study a company and pick up on their language. For instance, many people will choose a work password that relates to their job or company such as ‘company1234’.

This method is called spidering and is generally targeted at large companies with plenty of information about themselves online. Spidering is often used to gain access to Wi-Fi passwords as many office routers are protected by a password that relates to the company.

Spidering attacks consist of studying a company and picking up their language, e.g. company1234

How to protect yourself from cyber criminals

In its report, SplashData offers businesses the following advice to protect themselves from online hackers:

- Use passphrases of twelve characters or more with mixed types of characters.
- Use a different password for each of your logins so if a hacker gains access to one of your passwords, they won’t be able to use it to access other sites.
- Protect your assets and personal identity by using a password manager to organise passwords, generate secure random passwords, and automatically log into websites.

Protecting yourself from cyber criminals is a necessity

The convenience of cloud password managers

Password managers have become increasingly popular in recent years, offering a centralised way to store passwords.

They help you to generate strong passwords - you only need to remember a single master password. You type in your master password and gain access to all your other passwords that are stored in the cloud.

Password managers are certainly a step up from putting a post-it pad on your monitor or using 12345 as your password. But that same architecture puts an outright question mark on its security.

The risks of cloud password managers

While password managers may be convenient, there are three major flaws with this strategy.

First, you're reliant on one solitary barrier. With all your passwords centralised, your one master password becomes your single point of failure. If that master password is compromised in any way, you expose all your passwords. This leaves you in a highly vulnerable position.

Second, all your passwords are centralised in one location – along with everyone else's. Essentially, you're storing your passwords on the same servers as millions of other people. That's quite an appealing target for cyber criminals and hackers.

Third is the cloud itself. Servers get hacked, more and more. Would you leave your house keys on the cloud? No, you keep them with you.

A more secure approach to password management

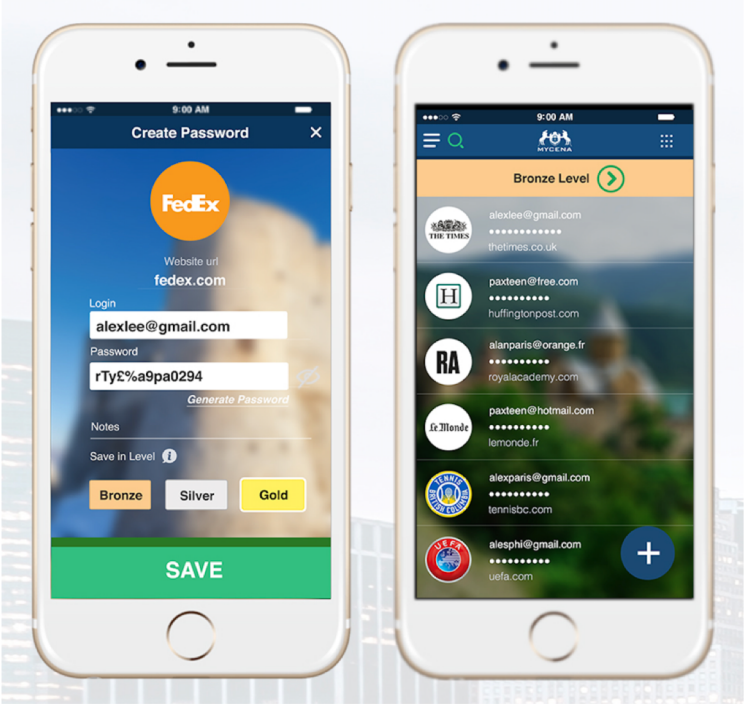
Rather than centralising passwords, MyCena is based on a fully distributed and decentralised risk model.

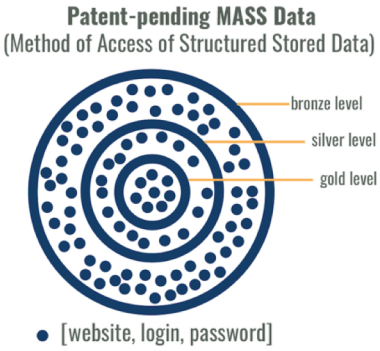
Instead of storing passwords in the cloud, passwords are encrypted and saved locally on your mobile device. With MyCena, all your passwords are stored under one, two or three levels of security depending on their sensitivity – this represents a huge step forward from being protected by just one master password.

Each user has a unique combination of fingerprints, pin, lock pattern, face ID and voice passphrase to access their passwords.

MyCena key security features

These are the three main features of MyCena:





MYCENA = MOST SECURE, MOST CONVENIENT

- No single-slick. No master password. **No leak propagation.**
- Keep 1000 encrypted passwords **in your pocket**
- Access securely from **anywhere**

1. There is no master password, instead you create a three-level security electronic vault inside the device.
2. Only you can access your vault with your unique identifications like fingerprints, face ID, voice passphrase or lock pattern. This ensures that if you lose your device, your passwords are safe, and you can reupload your backup onto a new device.
3. The key benefit is that you always have your passwords with you. And if ever your account email and password are leaked because of a data breach, your other accounts will remain unaffected.

Key Takeaways

If you're a Chief Information Security Officer, these are some key points to consider.

CISOs need to find a way to manage passwords that is secure but also convenient for their workforce.

- We all need to generate hundreds of passwords and remembering them becomes an impossibility.
- Many users still prefer the convenience of using predictable, easily discoverable passwords – ignoring the high level of risk this presents. Cyber criminals have been quick to take advantage of this situation, using flawed passwords to cause millions of pounds worth of damage to businesses.
- 4 out of 5 breaches are linked to passwords. To solve this problem, CISOs need to find a way to manage passwords that is secure but also convenient for their workforce. Yet password management only represented 0.53% of total cybersecurity spend in 2017, to increase to 0.58% by 2023.[1]
- Cloud password managers although convenient present major risks sensitive industries cannot ignore
- MyCena is a mobile application to help your staff access their passwords quickly and securely. Even if they lose their device, a thief wouldn't be able to access their passwords because the app is identity proof. It is an easy to roll out, cost-effective and highly professional way of ensuring password security without compromising efficiency or productivity.

1 Stratistics MRC https://www.strategymrc.com/report/password-management-market-2017 https://www.strategymrc.com/report/cyber-security-market https://www.strategymrc.com/report/cyber-security-market-2016
MyCena estimates

Discover more about MyCena

MyCena is a password security mobile application for smartphones and tablets.

Download from the Appstore or Google Play.

Companies can sign up for a free trial
on https://MyCena.co/business

For Enquiries

Contact support@MyCena.co

MYCENA
Protect Passwords