REDEFINING Password Security

By Julia O'Toole
Founder & CEO of MyCena Limited

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 are the keys which unlock the doors to our digital world. Just as our keys open the doors to our physical space, passwords open the doors to our digital space. They were devised to offer a simple way of proving our identity when using websites, email accounts and applications. Passwords are de facto our first line of defence against intruders.

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

Why passwords don't protect your doors anymore

But passwords are not doing their job anymore. In fact, a Verizon Data Breach Investigations Report shows that 81% of data breaches are a result of password failures, through either weak, reused or even stolen passwords.1

Why we still use high-risk passwords

Our increased reliance on mobile and web applications has led to a surge in the number of passwords. From simple email accounts to online banking, we are faced with hundreds of passwords to use.

While we know we need to use strong passwords, we simply cannot remember hundreds of combinations such as 45£@fag54hF8sD* to unlock each door. As a result, we tend to default to simple combinations like 'name1234' or reuse a single password with variations.

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

The top ten worst passwords of 2018

SplashData's annual list of Worst Passwords of the Year[2] reveals computer users are still using the same predictable, easily guessable passwords, despite the significant risk of being hacked and having their identities stolen. 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


A weak password is like having no password at all

In addition to this, the majority of us regularly use the following unsafe methods to store passwords:[3]

- 53% Human memory
- 32% Save in browser
- 26% Spreadsheets
- 26% Write it down
- 1% Other

1. Verizon Data Breach Investigations Report https://www.verizondigitalmedia.com/blog/2017/07/2017-verizon-data-breach-investigations-report/
2. SplashData's Top 100 Worst Passwords of 2018 https://www.teamsid.com/splashdatas-top-100-worst-passwords-of-2018/
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

Why passwords are a huge threat to businesses

How hackers operate

To understand why passwords are such a security threat, it is important to understand how hackers operate.

- Phishing – hackers can pose as genuine contacts, for example banks, to convince users to hand over their credentials.
- Social engineering – hackers extract information from your online profile and activities for identity theft.
- Credential stuffing – hackers typically use stolen account usernames and passwords from a data breach to try and open other accounts using web automation tools.
- Brute force – hackers run scripts to test credential combinations to 'guess' your password.

An alternative called spidering is when hackers study a company and pick up on their language. This is generally targeted at large companies with plenty of information about themselves online. It is often used to gain access to Wi-Fi passwords, as many office routers are protected by a password that relates to the company, such as 'Company1234'.

Over 90% of attacks are run by bots, which will 'stuff' or 'spray' tried and new combinations. These bots use leaked credentials and social media profile information to 'guess' faster. Most passwords can be cracked within 24 hours using a brute force tool that can be downloaded for free.

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

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

Why digital transformation increases vulnerabilities

While over 60% of Fortune 500 companies have gone through a digital transformation, enabling a more collaborative workforce, their connected networks have also become a hacker's dream. Their surface of attack is now the entire workforce. From chief executives to junior employees, anyone who is connected to the system is vulnerable to cyber attacks and poses a potential risk.

Meanwhile, business users' need for more and more accounts means they are more likely to reuse passwords across multiple accounts, increasing their risk of being hacked. On the other hand, companies using the convenience of Single Sign On (SSO) are vulnerable to hackers breaching their networks of information and databases from one access point.

It is therefore not a surprise that credentials thefts are on the rise. 2018 was the worst year on record for cyber security breaches. This was hotly followed by two of the largest leaks of usernames and passwords in history, named Collection#1[1] and Collections #2-5[2] in January 2019. There are currently over 3 billion logins and passwords up for sale online and this figure keeps rising every day.

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

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

Why new data protection laws affect every business

From small businesses to large corporations, every business in any industry needs strong passwords to protect their data and that of their customers.

With data privacy and protection laws like GDPR taking effect around the world, the financial consequences of failing to protect customer data and privacy can be devastating, as companies are now liable to fines of up to €20,000,000 or 4% of their total global turnover.

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

The risk of being a "big fish"

The hacking industry is made up of a wide range of actors, from unsophisticated criminals to nation-states. While some hackers cast their net wide, others concentrate on higher prize targets in more strategic sectors.

Breaches in sectors like defence, police, government, energy, water, utilities, infrastructure, technology, telecoms, universities, banking, financial services, healthcare, pharmaceuticals, transport, logistics, retail or law can have devastating effects.

In May 2017, the WannaCry ransomware attack led to the cancellation of 19,000 medical operations and appointments in the UK, costing the National Health Service (NHS) there £92m in disruption to services and IT1. And in September 2019, almost the entire population of Ecuador had their personal data leaked2.

When a "big fish" is breached, it inevitably also affects suppliers, partners and clients in turn. In March 2019, a Citrix data breach had the potential to affect virtual private network access and credentials to 400,000 companies worldwide including 98% of the Fortune 500 organizations3.

In the age of cyber warfare, there has been overwhelming evidence that some attacks are state-sponsored. Countries such as North Korea, Iran and China are notorious for conducting cyber-attacks and IP theft.

For example, the now defunct Canadian telecoms company Nortel was subject to a years-long attack, wherein hackers stole passwords from top executives to access emails, research, business plans and trade secrets. The attacks were later traced to state-sponsored hackers in China4.

The now defunct company Nortel was subject to a years-long attack traced back to state-sponsored hackers in China

Companies don't always realise there is a breach

Many businesses fail to recognise a cyber security breach when it occurs, with 93% of data breaches going undiscovered for weeks on end5 .

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 the company's network before the company even realises its security has been breached.

Data breaches can go undiscovered for weeks

1. Department of Health and Social Care https://www.hsj.co.uk/technology-and-innovation/cyber-attack-cost-nhs-92m-dhsc/7023560.article
2. The New York Times https://www.nytimes.com/2019/09/17/world/americas/ecuador-data-leak.html
3. Forbes https://www.forbes.com/sites/kateoflahertyuk/2019/03/10/citrix-data-breach-heres-what-to-do-next/#47a1e6b11476
4. The Register https://www.theregister.co.uk/2012/02/15/nortel_breach/
5. Verdict https://www.verdict.co.uk/password-security-surveillance-fears/

Does your business take cybersecurity seriously?

Businesses may have good intentions, but this is not always reflected in their practices. 74% of businesses and 53% of charities say that cyber security is a high priority for their organisation's senior management. Despite this however, we still see:

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

Balancing prevention, monitoring and remediation

With more and more attacks taking place every day, it is not a case of if but when your business will be targeted. There is a rising pressure on CISOs to mitigate ever more risks with limited resources. Approximately 99% of business cyber security spend is currently on monitoring and remediation. However, even the best monitoring and surveillance systems doesn't protect your business from password theft.

While 80% of the risks are related to passwords, password management only represented 0.53% of total cybersecurity spend in 2017, a figure forecast to increase to just 0.58% by 20232. To help protect their staff, clients and wider communities from security threats, companies need prioritize prevention and better organise their first line of defence.

How to prevent yourself from getting breached by passwords

A first step would be to set up an Identity Access Management (IAM) system that enables managers to assign different levels of access for different users within an organisation. This may not be the first consideration for smaller enterprises, particularly those who do not have a CISO.

A second step would be to set up a password management system that is both convenient and secure to prevent people from using weak or reused passwords. Many businesses fail in this area because they have a flawed password system, thereby increasing their risk of attacks.

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.

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
2. 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

Understanding the risks associated with centralised cloud-based password managers

Offering a centralised method of storing passwords, cloud-based password managers have become increasingly popular in recent years. This is largely because:

- 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.
- They provide a far more secure alternative to using post-its or weak passwords such as 123456.

A cloud-based password manager is convenient but risky

While cloud-based password managers may be convenient, there are three major risks associated with their architecture:

- First, by construction, all your passwords are centralised and accessed through one master password, which becomes a single point of vulnerability. Imagine if that master password is compromised in any way, you expose all your passwords at once. You can think of a master password like a hotel manager's key. A hacker only needs this key to access all the rooms. For many businesses, this is not a risk they can take.
- Second, all your passwords are sitting on the cloud, centralised, in the same basket as millions of other users' passwords. This becomes an enormous magnet for hackers, who are drawn like bees to a honeypot and will make every attempt to break in and rob the bank.
- Third, servers can and do get breached, whether through passwords or other vulnerabilities. Would you ever leave your physical house keys with someone you don't know? Then why do that with your digital keys? Leaving them on the cloud is effectively doing just that.

Your master password is like the key to the kingdom

Redefining the rules of password security

Redefining the rules of password security

A problem well defined is a problem half solved. To find a solution, we needed to break down the problem from scratch and rethink the rules that allowed passwords to fulfil their role as your first layer of security. We found three key rules :

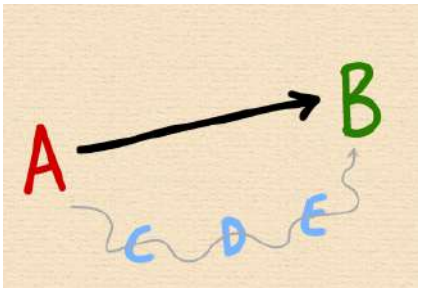
- Passwords are like keys. Just as you don't need to remember how to cut your keys every time you want to open a door, you should not need to remember your passwords to open your digital doors either.
- Passwords should be private by nature and only accessible by their owner and no one else.
- Passwords should not be vulnerable at a single point of access.

Lessons from neuroscience: understanding convenience

To achieve adoption and usage of any new technology, convenience is key. That rule applies to security. If it takes too long to open a door multiple times a day, most people will stop locking the door properly. Therefore, security can only be guaranteed if the systems and procedures that deliver it can be seamlessly applied.

In the last twenty years, neuroscience has taught us a lot about how our brain works. One key finding is that our brain tends to revert to the easiest path to travel from A to B. Here are just a few examples:

- When it comes to finding an object, it is much more efficient for the brain to remember a typical place where you ordinarily put that object rather than remembering precisely where the object is.
- It is easier for the brain to follow known or recognisable patterns than to create new ones. That explains why the brain is not so good at creating new random passwords.
- Our brain is visual and tends to match what it is looking for with objects and patterns seen before.



The brain tends to revert to the easiest path

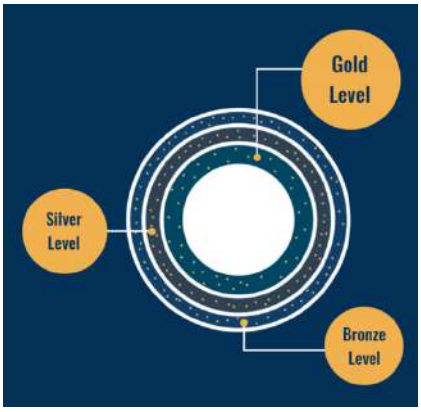
Making passwords work again

Having defined the problem, we still have to solve it.

International patent-pending Method of Access of Structured Stored Data (MASS Data)

Having defined the problem, we still have to solve it. MASS data is a breakthrough solution that allows passwords to be localised and decentralised, thus distributing and reducing the risk of losing everything at once. It allows the creation of multiple levels of security to store passwords depending on their sensitivity, with multi-level local authentication and full user control of passwords and security settings.

- No cloud storage.
- No master password.
- No single point of vulnerability.



MASS Data: local multi-layered password vault inside your device

Nail convenience to nail security

Cybersecurity is everyone's responsibility. To be widely adopted, the solution has to be fast, convenient and easy to use.

- Allow the owner of the passwords to prove their identity easily and safely at each level to access their passwords anytime, anywhere with a combination of fingerprint, face ID, PIN, lock pattern and voice passphrase.
- Generate strong passwords by default.
- Allow finding, copying and pasting of passwords without having to type, re-type, or see any given password.

Convenience is key - Create, save, search, find, copy and paste passwords in seconds

Building an enterprise-grade solution

To fit the enterprise environment, the solution needs to be easily deployed and used. It comes in two parts:

- A console through which a manager can quickly onboard all employees, strengthen and monitor password policies such as password length setup, password change frequency and weak password alerts.
- A mobile application employees use to access their passwords quickly and securely, that includes features such as multi-device, multi-platform, desktop integration, travel mode, synchronisation, migration, automated backup reminders and safe password sharing.

A console allows managers to strengthen password policies and monitor compliance

Respecting privacy by default

After many years of privacy erosion, lawmakers have strengthened privacy laws to safeguard our societies and individual liberties. We deeply support that trend. In fact, our solution is built with privacy by default.

Passwords are encrypted inside your device using AES-SHA 256 encryption. That means that even if you lost your device, a thief still wouldn't be able to access your passwords. The only person who can reupload your encrypted passwords backup is you.

Your biometrics data, like fingerprint and face ID, are even more sensitive. You can change a password but you cannot change your face or finger. All personal authentication is therefore kept inside your local device, with no central repository of biometrics on the cloud for anyone to steal.

Privacy by default: Never see or type a password again

Limiting damages caused by phishing

You may also never need to see a password again. That means, from the creation of your passwords to the use of your passwords through 'copy and paste', there never needs to be a moment where you have to show or type your passwords, limiting the chances of typing mistakes or having someone snooping behind you and stealing your passwords.

Even if a hacker manages to lure you to paste a password onto their fake site, thereby stealing it, that password cannot be reused to enter other accounts, since every single one of your passwords are unique and all are strong. Your entire network is therefore not exposed to any single break-in act.

Your first level of enterprise security

Once the solution is deployed inside an organisation, it becomes de facto its first level of enterprise security. To enter any password- protected application or network within a company, an employee will first need to prove their identity to their own device. Only then can they access the strong and unique password they are after. That strong and unique password will then prove that the employee has the right (because they have the unique key) to access that application or network.

The solution becomes your first level of enterprise security

Discover MyCena decentralised password security solution

Discover MyCena

MyCena Business Fortress is a revolutionary enterprise-grade password security solution that is decentralised, easy to implement, convenient and secure. Learn how to install and configure MyCena easily for your business.

MyCena Personal Fortress is a revolutionary personal passwords security application that individual users can download onto their mobile device. Learn how to protect your passwords using MyCena Personal Fortress.

MyCena as a Service

MyCena as a Service (MaaS) is a full service pack offering the best of the solution with advanced support, reducing the effort to implement and manage the solution within the corporation and its employees.

Key Takeaways

Cybersecurity is the number one threat to organisations. The number of data breaches is rising by the day, each bringing its toll of fines, legal actions and remediation while irreversibly damaging company reputation and customers' trust.

To protect their companies, boards and senior executives need to understand where the threats are coming from and take decisive action. As 81% of breaches start with passwords, password protection is no longer just an option, it is an imperative.

Companies' CISOs can mitigate risks by directing and helping their employees to use strong unique passwords as their first line of defence and decentralising password storage with MyCena Business Fortress. CIOs can also mitigate the risks of data breaches by taking advantage of MyCena as a Service.

For enquiries, contact
support@MyCena.co

Visit our website for more information
Free trial available
https://MyCena.co/business

Download from the Appstore or Google Play.