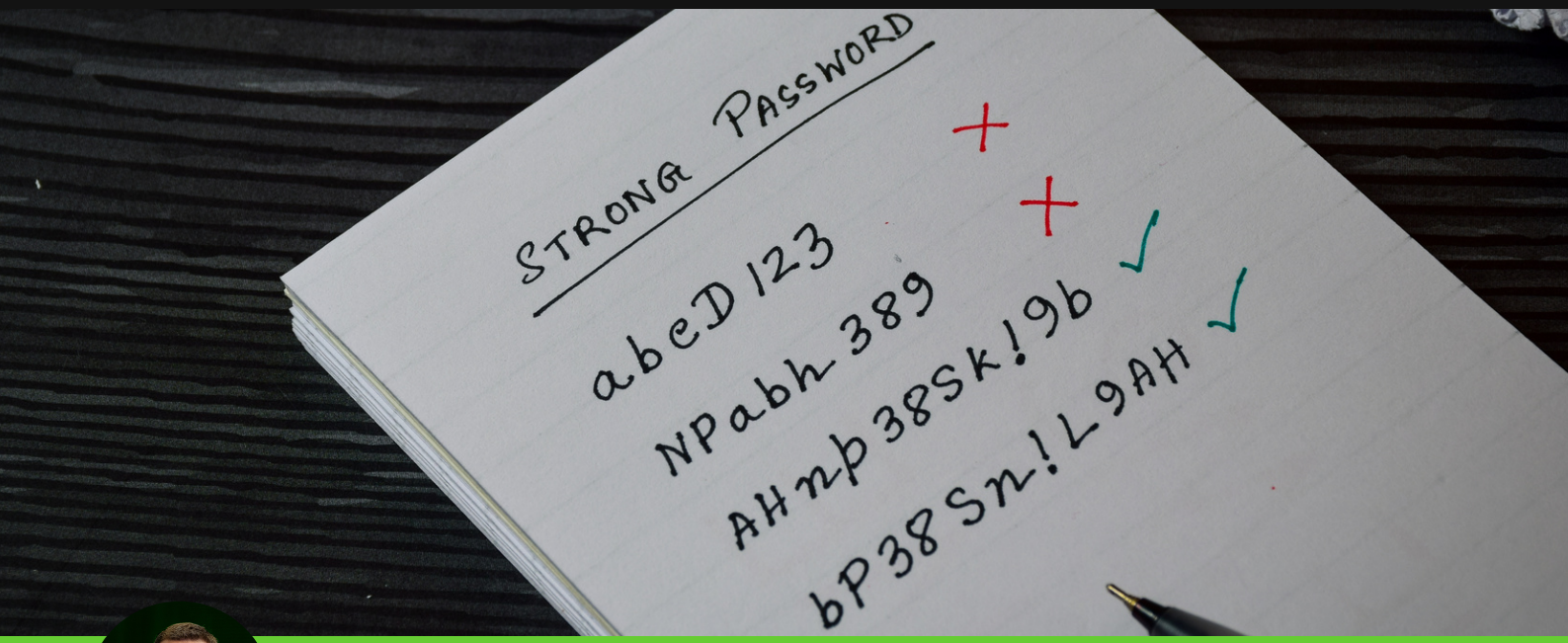
JANUARY 2023

inside zhero

Let's take a look at what is happening at Zhero



MESSAGE FROM IZAK

As 2023 gets underway, we all need to be particularly mindful of the influx of cybercrime that is taking down businesses left, right and center. In August last year, cybercriminals stole a backup of customer vault data from the password manager giant, LastPass. Two weeks ago, the workspace platform Slack disclosed a breach in their systems.

It seems that nobody is safe online from bad actors, especially with our passwords and logins being the most vulnerable. Zachary Quinto of Star Trek fame once said:

"I changed all my passwords. I have no two passwords that are the same for any service online. I have two-step verification enabled on all my devices...so yeah, I did take some extra steps that I hadn't taken before being exposed to this world."

in this issue of Inside Zhero we focus on what you can do to keep your passwords safe and become a password manager master. Happy reading!

Izak Oosthuizen
Bestselling Author and
Founder and MD of Zhero

BREAKING NEWS: NEW PARTNERSHIP WITH THE CRC

Team Zhero is proud to announce that we are now a Trusted Partner of the **Cyber Resilience Centre for London** (CRC). Our collaboration with the CRC for London was made possible with the initiative and support of Zhero's founder, Izak Oosthuizen, our Head of R&D, Professor Muttukrishnan Rajarajan and CRC CEO, Simon Newman. Zhero is one of only eleven IT providers to be elected as a CRC Trusted Partner.

Founded in 2022, the primary objective of the CRC for London is to provide cybersecurity advice and support for London-based businesses, with a focus on small and medium-sized businesses (SMEs). It is part of a national network of nine Regional Centres across the country whose role is to support SMEs and third-sector organisations to reduce their vulnerability to cybercrime. The CRC is a police-led, not-for-profit organisation working in partnership with the Mayor's Office for Policing and Crime.

The CRC's services include Security Awareness Training, Business Continuity Exercises and Vulnerability Assessment. Its Community Outreach programme involves visiting small business owners at their place of work. Working alongside uniformed police officers, practical support on improving cybersecurity is provided onsite. This includes step-by-step guidance on setting up two-factor authentication, automatic updates and implementing a robust password policy.

Team Zhero is super excited about the opportunities that this partnership has to offer. Each of the eleven CRC partners will be given a specific month to showcase their cybersecurity expertise, which Simon says is like being given the keys to the CRC for London. Zhero's turn is coming up in March. Working with the CRC, we'll be hosting events and live webinars, creating educational material such as infographics, and participating in the Community Outreach programme. Our alliance with the CRC for London forms part of our mission to make London a safe place for all to do business online.

A PERPLEXING PASSWORD PUZZLE

In this feature, we take a look at various aspects of password practice and management. These include testing the strength of your passwords and how to optimise password management practices.

WHAT DOES THE LASTPASS BREACH MEAN?

The LastPass 'security incident' may seem like old news but it will not be quickly forgotten. In December 2022, the password manager claimed that hackers had stolen both encrypted and unencrypted customer data, including encrypted password vaults. LastPass was adamant that the data was of little use to anybody without access to futuristic computing power and loads of time.

Nevertheless, the fiasco certainly provided us with plenty of food for thought about password security. If bad actors were able to penetrate the seemingly impenetrable LastPass with its military-grade encryption, two-factor authentication (2FA), mobile biometric login, and regular third-party audits, then what hope remains for secure password management? Are we destined to revert to post-it notes stuck under our keyboards? Will we need to change the way we do passwords?

LastPass was founded in Fairfax, Virginia in 2008. In 2009, the company was named 'Editor's Choice for password management by PC Magazine. In 2015, LastPass was bought out by LogMeIn, becoming independent again in 2021. LastPass employs 550 people and has an annual revenue of about $200 million.

Including the breach announced in December last year, the password manager has had a total of eight security incidents, many relating to web extension vulnerabilities.

LastPass

HOW STRONG IS MY PASSWORD?

In 2021, the password '123456' was voted the worst and most commonly used credential in the world, no different from the situation in 2010. It's no wonder then that hackers find passwords easy pickings. Verizon Data Breach Investigations reported that 81% of all data breaches are caused by the compromise of weak passwords. The situation is exacerbated when the same password is used across multiple sites or accounts.

So how can we determine if a password is weak or strong? A simple solution is to use an online password strength checker like How Secure Is My Password.

This table compares a password with the time it would take for a cybercriminal to crack it.

PASSWORD	CHARACTERS	TIME TO CRACK
apwmlq	6	9.6 seconds
apwmlqr	7	8.33 minutes
apwmlqrd	8	3.6 hours
apwmlqrdc	9	3.91 days
apwmlqrdcv	10	7.16 years
apwmlqrdcvt	11	160 years
apwmlqrdcvtz	12	9 millenia

The long and the short is that the longer your password and the more character sets you use, the more difficult it is to crack. **Click here** and test how strong – or weak – your passwords are.

WHEN PASSWORDS ARE STOLEN

When passwords are stolen, the consequences can be dire. Hackers use various methods to steal passwords, including phishing scams, malware, and keyloggers.

One method used to steal passwords is brute force attacks. A brute force attack is a method of guessing a password by trying every possible combination of characters until the correct one is found. This method is often used when hackers have obtained a list of email addresses and passwords from a data breach.

To protect yourself from brute force attacks, it is important to use strong and unique passwords for each of your accounts and to enable two-factor authentication. If you suspect that your password has been stolen, it is important to change it immediately and monitor your accounts for any suspicious activity.

BAD NEWS FOR BUSINESS

For businesses, the situation is even worse. IT Governance confirms that stolen passwords are one of the simplest and most common causes of data breaches in the corporate world. Others include application vulnerabilities, malware, malicious insiders, and employee error.

According to IBM, these are just a few of the costs incurred if your network is breached due to weak passwords:

- the average cost of a data breach is $4.2 million
- lost opportunities average out at $1.6 million
- 39 % of costs are incurred more than a year after a data breach
- it takes about 280 days to identify a data breach
- containing a data breach takes about 80 days

If those numbers aren't bad enough, your business will also suffer irreparable reputational damage, high employee turnover, and increased cyber insurance premiums. And here's some food for thought from cybersecurity expert Ted Schlein:

"There are only two different types of companies in the world: those that have been breached and know it and those that have been breached and don't know it."

HERE TO STAY

Passwords aren't going to die anytime soon and we surely can't backtrack to the days of Post-it notes. Replacing passwords with biometric data, such as fingerprints and face-scanning technology, is still a work in progress. In the meantime, we are stuck with the trusty and frustrating password. We've all heard supposed 'good' password policy advice ad nauseam.

REFINING PASSWORD MANAGEMENT

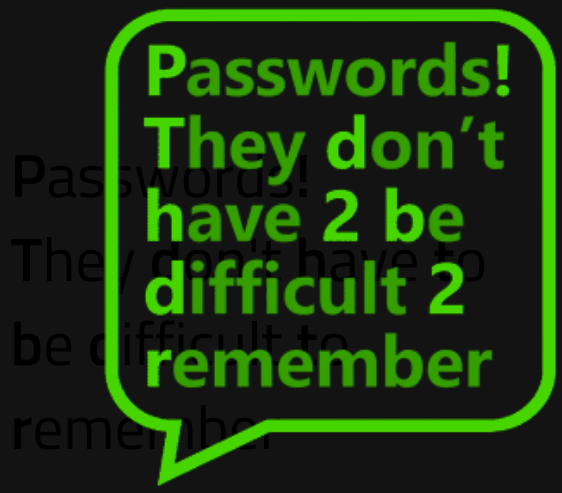
Derek Smith, Founder of the National Cybersecurity Education Centre in the United States, recommends these strategies to help you achieve the best password practice:

- create long and strong passphrases of up to 64 characters
- apply non-reversible end-to-end encryption to passwords which will protect them in transit over a network
- test your password using online tools
- avoid dictionary words that can be hacked by dictionary attack software
- use different passwords for different accounts
- avoid changing your passwords every 90 days as you'll probably end up using a similar password
- only change passwords in case of a perceived threat or an actual data breach
- change passwords when staff leave so that disgruntled employees can't meddle in your business – or destroy it
- remove permissions of applications when you don't need them anymore
- use up-to-date anti-malware and vulnerability management solutions

PASSPHRASES

Passphrases are long passwords that can be up to 100 characters or more in length. Passphrases are customised and therefore often easier to remember than long passwords.

It is possible to use only words for passphrases but most software, applications, and services only accept those with a mix of letters, numbers, and special characters. Passphrases are much more secure than passwords. Some say that the NSA would find good ones impossible to crack even using the most sophisticated brute-force software.



A PLACE FOR PASSWORD MANAGERS?

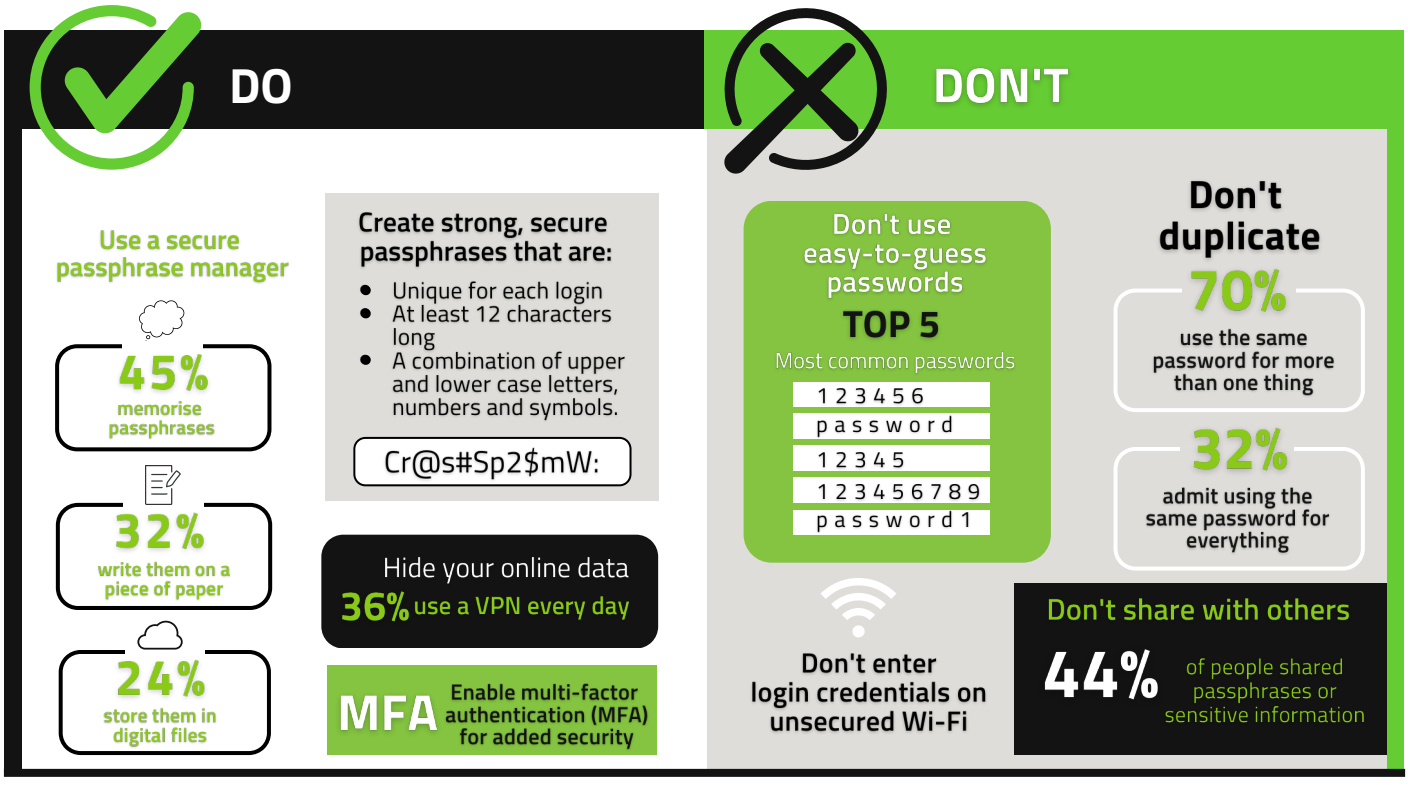
Despite being a cybersecurity guru, Derek Smith does not hold any grudges against LastPass. He still believes that LastPass and other password managers offer superlative security when it comes to protecting your logins. Password managers are convenient since you only need to remember your master password – they store the rest for you. They also generate and save strong, unique passwords when you sign up to new websites.

Despite the LastPass debacle, Smith thinks that password managers are designed to provide you with access to all your passwords in an encrypted format that is not accessible to hackers or malicious software, thereby ensuring that your data is always private. And LastPass doesn't have a monopoly on password management. There are a number of password managers on the market, including the Zhero Vault.

PERFECTING YOUR PASSWORDS

Optimising your password practice shouldn't end with passphrases, end-to-end encryption, and password managers. Multi-factor authentication (MFA) aka two-factor authentication provides an additional layer of security so that cracking a password is simply not enough for a hacker to gain access to an account or network.

Besides traditional credentials, such as your username and password, MFA mandates users to confirm their identity with a one-time password (OTP) or code sent to a mobile device or using a personalized security token like a USB or a smart card. You can even take MFA one step further by adding advanced authentication methods and leveraging biometric verifications. For example, Windows Hello on Windows 11 means that employees can be identified by recognizing their faces, fingerprints, voices, irises, or even heartbeats.



VIN MEETS THE LORD MAYOR OF WESTMINSTER

Vin recently had the pleasure of meeting the Right Worshipful Lord Mayor of Westminster along with some other Mayors from London boroughs. They all came together at a networking event held by the Kensington, Chelsea, and Westminster Chamber of Commerce.

Inside Zhero: Can you tell us about your recent meeting with the Lord Mayor?

Vin: It was an incredible experience to meet and speak with Hamza at the annual Christmas lunch at the Royal Garden Hotel. Not only was it a great opportunity to connect with him, but we were also able to raise £3,000 for charity. It was a great all-around experience.

Inside Zhero: Can you share more about your interaction with the Lord Mayor?

Vin: I found it to be a very productive meeting. Hamza and I had a lot in common, including attending the same university. He had some interesting ideas about providing opportunities for underprivileged youth in the technology industry. It's impressive that he's the youngest ever Lord Mayor of Westminster at only 22 years old.

Inside Zhero: That sounds like a valuable meeting. What's next for Zhero?

Vin: I plan to explore ways to gain new business opportunities through the Lord Mayor and future events with the Chamber of Commerce. I have been involved with the Chamber for 25 years as a past Chairman, President and current Board Member. I believe there are many exciting opportunities for Zhero in the future.

MICROSOFT LICENSING

Please note that as of the 1st of April 2023, the cost of your Microsoft Licensing will be increasing by 9%. Microsoft has also confirmed that this increase is to apply at 6 month intervals for the foreseeable future.

OUR AMAZING TEAM

IT'S BEEN 6-MONTHS ALREADY?

We are pleased to announce that 3 members of our team are celebrating their 6-month workiversary at Zhero this month!

Vin Jauhal

Vin, our Transition Coordinator, joined the Zhero team in July when we acquired Wem Technology. Vin has over 25 years of experience in the IT support industry, with extensive knowledge of operations, finance and projects. With his experience and contagiously good mood, Vin is an exceptional networker and a fantastic team player. We love having Vin on the team as he is always willing to help, motivate others and share his knowledge to upskill everybody.

Martyn Greville-Giddings

Martyn joined Zhero with a scorecard of 10/10, bringing to our family 20+ years of experience and a wealth of IT knowledge. Also coming over from the Wem acquisition, Martyn is very happy to have stepped away from first- and second-line support and is now focusing on infrastructure.

Kannan Govindaraj

Kannan brings more than 5 years of knowledge and experience in network support to the team. He forms part of our Projects department with a solid focus on supporting clients onsite. We all enjoy having Kannan around because his positivity puts everybody in a good mood.

Happy 6-months guys!

JOIN OUR AMAZING TEAM

THINK YOU HAVE WHAT IT TAKES?

We are always on the lookout for top talent. If you have what it takes to help us shift the dial up a notch, stay in touch for exciting opportunities.

Cape Town, South Africa

Account Manager

If you enjoy working with clients and giving them the best customer experiences, we are looking for you!

APPLY HERE

Interns

If you are a keen learner and looking to enter a dynamic IT company then look no further!

APPLY HERE

Service Desk Team Lead

We are looking for someone with a strong technical background, who is passionate about working with people and is ready to take the next big step in their career.

APPLY HERE

London, United Kingdom

On-site Engineer

We are looking for someone with a strong technical background, who is passionate about working with people and is ready to take the next big step in their career.

APPLY HERE

MEET THE TEAM

Clinton De Klerk

SERVICE DESK ENGINEER

1. What made you realise you want to go into the IT industry?

Being a gamer, I grew up behind a computer - I guess this is where my love for technology started. Technology is also a dynamic industry and always changing. I am constantly being challenged and I enjoy that - never a dull moment!

2. What's your most-used productivity tool?

My laptop and my work ethic.

3. What do you enjoy the most about your job?

I enjoy learning new things every day. I love resolving IT issues for clients. It makes me feel like a superhero at times.

4. How would you describe yourself?

I am calm, quiet, and reserved. I am always willing to share my knowledge and help others. I can be funny sometimes.

5. Where will we find you over weekends?

I am a family man - over weekends you find me spending time with my family.

6. Do you have any hidden talents or hobbies?

I do enjoy a game of pool.

7. Are you a sports fan?

I am not a big sports fan, but I enjoyed watching cricket as a kid when growing up. I still enjoy watching big matches with friends and family.

8. What is your favourite series?

Enjoy am hooked on Queen of the South and I love watching crime documentaries. I am also a big reality TV fan.