FEBRUARY 2021 | PRODUCTIVITY ARTICLE 2

# PASSWORD MANAGEMENT: PROTECTING SENSITIVE DATA WITH THE RIGHT TECHNOLOGY

*By Rowan Caffull*

I am an unapologetic and passionate lover of tech. It's something that feeds into both my personal and professional life. While my role at Chambers certainly doesn't sit within IT support, I have unintentionally gained the reputation as somewhat of a 'fixer'. Over the years, I have happily waded through many a distressed call from fellow colleagues. At times, Google has been my trusted advisor and, at others, I have jumped off the back of my own experience.

It may (or may not) come as a surprise to some that the most common queries I've received over the years are those related to passwords.

*'Do you know what my password is for X?'*

*'How do I access this data without my password?',*

*'Can I change my password easily to get this document right now?'.*

Unfortunately, the powerhouse that is Google was rendered nearly obsolete in these instances. And while our skilled IT team could largely find ways around such problems, it remains abundantly obvious that password-related tech issues are going nowhere fast. We live in a world where nearly every application requires you to register, sign in or log on. Without this vital code, many of the documents and information that we rely on so heavily remains stored in a digital black hole - unattainable without the support of seasoned professionals.

One thing that hadn't passed my notice was the fact that these requests seemed to flood in right before timely events. Remote hearings or urgent deadlines were largely the moments where one came to the damning realisation that this code was no longer logged in their memory. And with many of us owning numerous email addresses, the issue becomes more complex by the second.

## Password lifespan and maintaining security

For many, the problematic nature of passwords comes down to something known as 'password expiration'. We may create an account with a memorable word and numerical configuration. We may even sit comfortably in the knowledge that said password has been etched clearly in our memory. However, these programmes create a requirement that forces users to change their codes every few weeks or months. The reality of this is that security actually becomes hindered as people turn to manual and makeshift ways to remember the 10th new password they've had in a working year. I've lost count of the number of times I've seen laptops with Post It notes, reminding the user of their password. Or the number of people that approach password expiration by creating patterns (password1, password2, etc…).

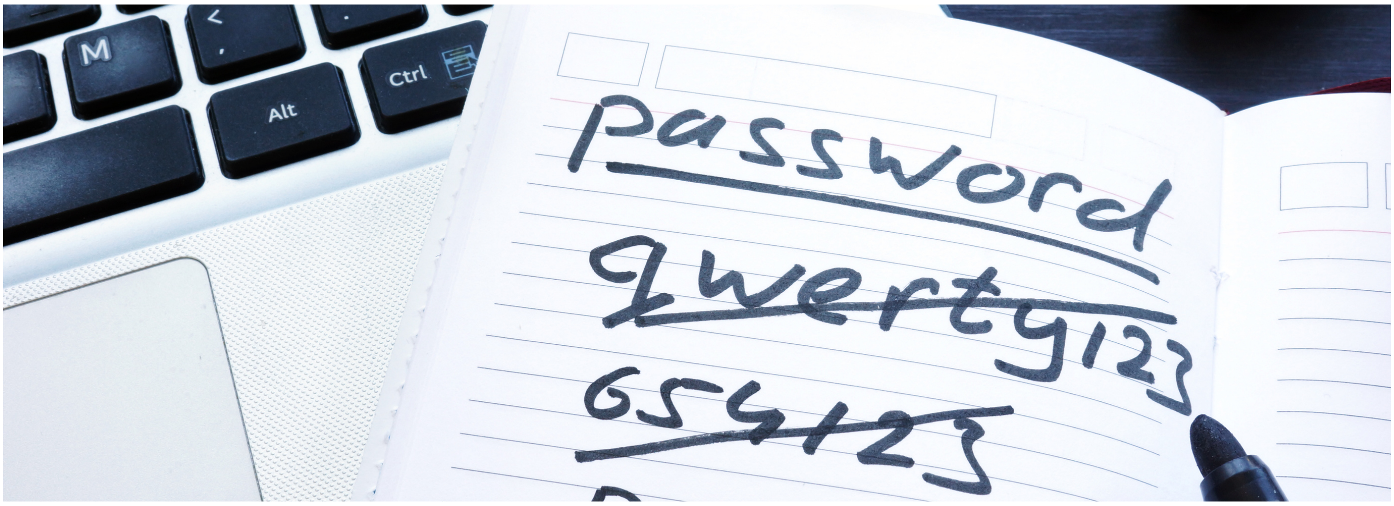
IT professionals have long been calling for a rethink of mandatory changes for password security. The thought is that it is better to have one ultra-secure password rather than an insecure one that renews every month. And this is where password managers come into action.

## The benefits of password managers in professional settings

Password managers have risen to popularity in recent years. However, regardless of the reassurance from a security standpoint, there is still a reluctance to take them on board. On the surface, you essentially pass over the login information for all of your sensitive data and protected services to an external party. There needs to be a degree of trust that this information is being kept secure and has been encrypted to prevent hacking.

Back in 2013, I set up my very first password manager. This manual process, I envisioned, would be a central storage place for around 20 applications including emails, socials, work tools, and online shopping accounts. To date, I have logged near to a staggering 400 passwords in my vault. An astronomical number of unique codes that would have no place in my memory, let alone when you take into account different emails and applications.

For me, **LastPass** is the best password manager available on the market. The zero-knowledge security model means that LastPass does not have access to your master password. They are



also restricted from gaining access to the data stored within your vault. All data is encrypted at the device level with AES-256 encryption - a symmetric key encryption that is regarded as one of the strongest standards available to date. It is then synced with TLS through a private connection to protect it from hackers.

Additionally, it runs security challenges to ensure your passwords are secure and not duplicated on more than 1 site. Any issues identified are flagged to you, giving you the option to manually change a password or have LastPass issue an automatically-generated secure one on your behalf.

In practice, this means that every morning, the first application I log in to is LastPass. One password to remember. 2-Factor Authentication (2FA) then requires me to authorise access using my phone. And from here, whenever I visit a website that requires me to log in, LastPass automatically does this on my behalf.

## Security benefits for the legal sector

The primary concern people flag with password managers comes down to one single point of failure. Namely, 'What if LastPass gets hacked?'. On this note, it's important to remember that password management companies are entirely devoted to online security - it's what they do day in and day out. If there is anyone who knows how to keep a password secure and away from the prying hands of a hacker, it's going to be them.

With the security benefits of password managers hailed across the internet and Multi-Factor authentication becoming standard, the need for password expiration policies and insecure passwords decreases daily. Beyond the purpose of security, these tools are designed to enhance efficiency. Remove the need to remember numerous passwords and you remove the burden on the IT department, potential delays in submitting work, and frustration at not being able to access relevant data.

At The 36 Group, we are encouraging all members and staff to embrace password managers. I truly believe that this should and will become standard practice for all, both on a personal and professional level. For now, however, I am simply happy that I can rest easy knowing that none of my passwords contain the word 'password' or number combination '123'.