Unsplash © Paulius Dragunas

Is the power of the password now dead?

As multi-factor authentication becomes the norm, plus the new security environment the pandemic has delivered, will passwords finally be consigned to history?

According to research from *LastPass*, 47% of respondents to their global survey did not change their online security habits since they began working remotely. Moreover, only around a third (35%) of employers ensured their workers changed their passwords frequently.

“Our latest report showcases the impact of the COVID-19 pandemic amid the increased time we spent online – which has in turn, increased our vulnerability to potential hackers,” said Dan DeMichele, VP of product management for LastPass.

“As we continue to grow our online presence, we need more robust protection for our online information. One way to combat this is by investing in a password manager which can be used to store your personal and digital information safely. As a business or IT lead, adding an additional layer of security, including multi-factor authentication or single sign-on options, will help to ensure that your employees are the only ones accessing their information.”

In recent years, companies have increasingly put pressure on their employees to maintain vital password hygiene, using strong, unique passwords for every account and not falling victim to phishing attacks.

> *But unfortunately, organisations set themselves up for failure by placing the onus on employees.*

According to Julia O'Toole, CEO and founder of *MyCena*, businesses must rethink their approach to digital security and retake control of digital access points. Instead of negating responsibility for their own cybersecurity, business leaders should take password creation out of the hands of employees entirely and eliminate the threat of phishing in the process.

Proofpoint's 2022 *State of the Phish* report revealed that 42% of employers inflict monetary penalties on staff that engage with actual or simulated phishing attacks in the UK, and 29% even lay off staff. These figures are both far higher than the global averages at just 26% and 18%.

Unsurprisingly, the report also highlighted an increase in the number of attacks year on year. For example, 91% of respondents revealed that they had faced phishing attacks in the UK, and 84% reported seeing at least one email-based ransomware attack.

"Instead of forcing employees to remember dozens of complex passwords for various access points, adapt your technology to support employees in only using strong unique and encrypted passwords that can't be phished," O'Toole concluded. "Not only do you take back the control of your own access points and cybersecurity, but you also relieve your employees from immense mental pressure. Information like passwords doesn't need to be kept in people's heads."

In addition, speaking to Maddyness, Jeff Shiner, CEO of 1Password, also explained that balancing convenience with business needs is the key to solid security: "For businesses, the benefit of Universal Sign-On is that it's going to be key for company-wide security. In addition, it will help with the trend of Shadow IT and the plethora of cloud apps that are emerging to help people with their productivity.

"Overall, taking a human-centric approach to security will be crucial as we continue working towards making it easy for people to stay secure online. By making it simple to stay secure at the individual level, you can protect them wherever they are (whether at work or home) and, by way of that, businesses will remain protected as well."

Unsplash © Franck

Skin deep ID

For many, *biometric-based* security should have sounded the death knell of the password. However, much like the paperless office, a password-free world has yet to materialise. The rise of multi-factor authentication is fast becoming commonplace, but even these advances won't consign the password to the history books.

"Multi-Factor Authentication (MFA) and authentication are always going to be core requirements for accessing any online account or other resources," says Alan Calder, CEO of GRC International Group. "In reality, passwords will be with us for the foreseeable future.

"Where passwords are concerned, what matters is complexity and uniqueness – which highlights the need for password managers. The effective use of password managers combined with more widespread deployment of MFA (particularly to high value accounts) will lead to reductions in personal data breaches."

What is needed is a multi-layered approach to digital security that factors in the use of passwords with other forms of identification. Increasingly, this means mobile devices with biometric identification systems already built-in. However, these services must be integrated with company-wide security policies that define good security behaviour.

"Businesses should have a strong password policy and require employees to do online self-paced security training," Neil Riva, principal product manager at JumpCloud, explained to Maddyness. "The training needs to cover the what and the why and include best practices and examples.

"Small businesses, in particular, face problems because the default tools that exist have often been built for the enterprise rather than smaller organisations. If you approach this from an SMB mindset, the actual problem is how to make this easy so that a small team can deliver the best possible service and keep things secure."

Strong security is integrated and multi-layered, using several tools to deliver robust security environments business leaders can rely upon. Creating these environments requires the cooperation of everyone that comes into contact with sensitive data.

Andrew Shikiar, executive director of the *FIDO* Alliance, said: "While more robust authentication methods like biometrics are gaining popularity among users, valid passwords remain most common. Put simply, passwords are so engrained in the fabric of our digital lives, to eradicate them totally requires

considerable effort for both organisations and consumers.

“Thankfully, the technology already exists to make passwordless a reality. Developed by some of the world’s biggest tech organisations including Apple, Google, and Microsoft, FIDO standards are highly secure and freely available – and are built into every leading device and web browser. The stage is now set to see more rapid adoption, as we’ve seen from companies like eBay and Microsoft which are enabling hundreds of millions of users to ditch their passwords.”

Seamless security

“Our data also tells us what to expect in the fraud landscape in 2022 and beyond,” claims the 2022 SpyCloud Annual Identity Exposure Report. “Reused passwords have been the *leading vector* in cyberattacks in the last few years.

> *“Users’ growing propensity to recycle their passwords, especially as they spend more time online, will further improve the cybercriminals’ odds of successful attacks.”*

Findings from the ‘*Hiding in Plain Sight*’ research report from 1Password found that one in four (25%) employees at IT/DevOps companies have secrets in ten or more different locations and have shared them with colleagues via insecure channels, such as email and Slack. Additionally, 61% of projects are delayed due to poor secret management, and one in three (36%) IT/dev ops workers say they will share secrets over insecure channels to increase productivity and speed.

“Developers encounter a lot of complexity when building and deploying secure software, and it can often seem like security and convenience are irreconcilable,” said Akshay Bhargava, chief product officer and GM of emerging solutions at 1Password. “1Password developer tools aims to make their lives easier by making complex security processes more convenient, and making doing the secure thing, the easy thing.”

And does the password have a future? Etay Maor, senior director of security

strategy at Cato Networks, concludes: “Passwords are not going away, but they are slowly morphing into more secure and easy to manage versions of themselves. For example, the classic static password is now augmented, in many cases, by multi-factor authentication. In addition, new solutions that rely on behavioural patterns are incorporated to identify and authenticate users. This means that the classic usage of passwords as an authentication tool is now changing to an identification tool.”

The security landscape has changed for many businesses and organisations. As the threat perimeter has shifted as remote mass working becomes the norm, the password will be joined by other security parameters to combat the changing threat actors and attack vectors businesses must protect themselves from as they move into the post-pandemic phase of their development.

Article by DAVE HOWELL