advance

PASSWORDLESS WHAT DOES THE FUTURE HOLD?

INTRODUCTION

Passwordless authentication is accelerating quickly, especially now that Google, Apple, and Microsoft have fully committed to this future[1] by agreeing to adopt passwordless standards and implement it in the near future. It's well known that few users of any system follow password best practices, and modern malicious attackers have advanced password-cracking techniques at their disposal. As large leaks of password databases become more common, weak and repeated passwords present a growing issue for businesses, while password volume and complexity have becomes a growing frustration for users.

Passwordless authentication aims to solve these issues by removing the need to remember login information, while maintaining a high level of data security. In a passwordless system, users prove their identity using one or more methods like biometrics and one-time codes.

[1]https://www.apple.com/newsroom/2022/05/apple-google-and-microsoft-commit-to-expanded-support-for-fido-standard/

THE PASSWORD PROBLEM

We're quickly moving away from the days of passwords scribbled onto sticky notes and towards one-time authentication codes. Passwords haven't changed much since the earliest days of computing[2], back in the 1960s. They still require the user to create a unique combination of numbers, letters, and special characters and then recall said combination during login.

Passwords worked relatively well when users only had a few accounts, but research in 2020 revealed that the average user had 150 online accounts[3]. It's impossible to remember 150 unique, strong passwords without recording them somewhere. And this number was expected to grow to more than 300 by 2022.

Most internet users do not follow proper password protocol. In other words, they repeat passwords across multiple accounts or use weak passwords with easily cracked words and number combinations. Cybersecurity experts outline a hefty list of requirements that make a password secure[4], but few follow them all:

- Choose a password that is 12-15 characters long.
- Don't use words, names, places, or other easily recognizable terms. These make passwords significantly easier to crack.
- Don't use sequential numbers; instead, randomise the order of numbers and letters with no discernible pattern.
- Do not reuse the password on any other account.
- Don't write the password down anywhere. But write down a hint that will jog your memory.

While these rules make great sense from a cybersecurity standpoint, they result in passwords that are very hard for humans to remember. When we factor in the number of passwords the average user has, the task of remembering them would become impossible.

Password management software does go some of the way towards improving this situation, but truly passwordless authentication solves it entirely.

[2]https://www.wired.com/2012/01/computer-password/
[3]https://blog.dashlane.com/world-password-day/#:~:text=According%20to%20our%202017%20findings,will%20skyrocket%20to%20300%20accounts
[4]https://www.webroot.com/us/en/resources/tips-articles/how-do-i-create-a-strong-password

HOW BIG OF A PROBLEM?

About 42% of Australians report repeating the same password for multiple accounts[5]. And 17% of those use the same one or two passwords for everything they do online. This creates a significant opportunity for malicious actors, who can easily find a user's password for a previously breached system, then test if it has been reused in other areas. Compromised accounts are the number-one cause of data breaches, with 80%[6] originating from stolen or lost credentials.

The website haveibeenpwned.com, which maintains a database of leaked credentials, has recorded more than 11 billion username and password combinations that have been published on both the normal and dark web.

IT professionals everywhere are already onboard and ready to say goodbye to passwords for good. 95% of Australian IT leaders[7] are concerned about the risks associated with user-generated passwords, and 100% note the benefits of going passwordless.

[5]https://www.proofpoint.com/au/corporate-blog/post/world-password-day-42-australians-reuse-passwords-across-online-accounts
[6]https://www.verizon.com/business/resources/reports/dbir/
[7]https://securitybrief.com.au/story/new-research-shows-global-drive-for-passwordless-authentication

WHAT IS PASSWORDLESS AUTHENTICATION?

Passwordless authentication is the emerging solution to the password problem. It refers to all the ways users can prove their identity other than a traditional password—removing the requirement for users to remember any passwords at all.

5 AUTHENTICATION FACTORS

Authentication factors can be divided into five types, of which all passwordless methods use one (or more!). Factors are the different categories of evidence users must present to prove their identity:

1. Possession Factors

A possession factor is something users have on them; typically their smartphone, but it can also be a dedicated hardware authentication device. When creating an account, users will link their phone or another possession factor. Each time they log in, they must prove they have this linked possession factor, usually through a one-time password sent directly to the device[8].

2. Inherence Factors

Inherence factors require users to present something unique to that user. Biometrics are a great way to verify identity because the chances are low to non-existent that a malicious attacker has the same biometric information to pass a facial, fingerprint, or retina pattern scan.

3. Behaviour Factors

Behavioural biometrics is a newer authentication factor that is continuing to develop[9]. Applications can learn particular behavioural characteristics unique to each user, such as typing habits, gait, cursor movements, and more.

4. Knowledge Factors

Knowledge factors include passwords, PINs, secret question answers, and other information that users must recall to verify their identity. As previously noted, knowledge factors aren't secure and are frequently misused. Knowledge factors shouldn't be used alone10 but are often combined with other authentication factors.

5. Location Factors

Location is not used on its own because it lacks specificity, reliability, and accuracy[11] but is combined with other authentication factors. Applications track a user's location trends (if the user has enabled location tracking) and will prompt additional authentication requirements, such a user's possession factor, when they try to log in from a new location.

[8]https://www.sumologic.com/glossary/authentication-factor/
[9]https://www.systancia.com/en/behavioral-biometrics/
[10]https://proofid.com/blog/knowledge-factors-possession-factors-inherence-factors/
[11]https://medium.com/os-techblog/is-location-an-authentication-factor-9ed33d633993

HOW ARE AUTHENTICATION FACTORS USED?

Two-factor authentication (2FA) and multi-factor authentication (MFA) are increasingly common, and most readers will already be very familiar with them. Instead of using a single knowledge factor, like a password, multiple factors combine to prove the user's identity. 52% of Australian consumers are more likely to sign up for an app or service[12] if the company uses multi-factor authentication (MFA).

For example, when a user attempts to log in into their account, a one-time password (OTP) is sent as a text, phone call, or email. Modern Android and Apple smartphones automatically recognise OTPs and will autofill passwords within smartphone apps.

Authentication factors are also used with single sign-on (SSO) technology[13]. SSO is prevalent in business settings because it allows users to log in once and access the organisation's entire suite of tools. Users must still authenticate with multiple factors, but once the authentication token is created, it is reused during that session for any application the user needs to access.

[12]https://itbrief.com.au/story/auth0-survey-reveals-australian-businesses-fail-to-meet-login-expectations
[13]https://www.cloudflare.com/learning/access-management/what-is-sso/

HOW CAN PASSWORDLESS TECHNOLOGY IMPROVE BUSINESS?

So passwords are bad. They pose a security risk and are an all-around hassle for users, businesses, and IT admins. But what are the implications for small and mid-sized businesses? Keep reading to learn five ways that passwordless authentication can improve business.

1. User Experience

User experience matters; if users don't feel good about the products they're using, they'll take their business elsewhere.

Passwordless authentication provides a frictionless login experience, as users will no longer struggle to recall passwords for each online account or be forced to reset a password they've forgotten.

Software developers stand to grow their customer base, increase customer satisfaction, and differentiate themselves from competitors by offering a seamless login experience.

Businesses outside the software space improve employee retention by using SSO and passwordless technologies to improve the employee experience. And as passwordless authentication becomes more commonplace in widely adopted consumer services, such as Facebook, Gmail and Apple services, it will increasingly become an expectation in the working environment as well.

2. Increased e Commerce Conversion Rate

User experience leads right into conversion rate. Users hate a hassle when trying to make purchases. And conversion rates are challenging to begin with; even top websites only get 5% of users to finish a session by checking out their cart[14]. Every barrier a business puts between users and checking out reduces conversion rates. When an ecommerce site requires a user to stop the checkout process and create an account, 24% of users abandon their cart[15]. Another 17% will abandon if the process is too long or complicated.

By going passwordless, users can quickly make an account and verify their identity using multi-factor authentication. Bridging the gap between consumer expectations and experiences is key to increasing sales and growing.

[14]https://www.wordstream.com/blog/ws/2014/03/17/what-is-a-good-conversion-rate
[15]https://baymard.com/lists/cart-abandonment-rate

3. Improved Security

Businesses are ethically responsible for protecting and securing any data they collect[16] from their users. Consumer data – from personal details to engagement and behavioural data – is collected for many reasons. But it's a challenge for businesses trying to keep user data safe. The current cybersecurity landscape is becoming more and more challenging, with more and more data breaches every day. Every week, over 1 million passwords are stolen and stored[17] by malicious actors.

Implementing passwordless authentication puts this problem to bed and greatly reduces intrusion risks as historic password breach databases and prevalent methods of password cracking are rendered useless.

4. Improved Productivity and Less Support

Password-related enquiries are a major contributing factor to the cost of IT support[18], often making up 20-50% of inbound support requests. Users are often unproductive or completely unable to work while waiting for their passwords to be reset. While passwordless technology is not without support requirements—some users will still need help if their possession factor needs to be replaced, or gets lost or stolen—the support requirements and downtime for users are greatly reduced.

Implementing passwordless technologies lets users be more productive, while IT resources and budget are freed up to support other business or cybersecurity initiatives.

5. Internal Systems

Consumers aren't the only ones who need to authenticate their identities. Employees are potentially even more of a risk than consumers because they can access a business's stored confidential, sensitive and personal information. Unfortunately, most employees struggle with up-to-date cybersecurity habits to protect confidential business assets. A report by My1Login found that roughly 66%[19] of employees reuse their personal account passwords for work accounts.

With passwordless authentication, IT can assign employees their appropriate privileges to confidential assets[20] without worrying about weak passwords. Password-stealing methods such as phishing are much less effective with passwordless administration controls.

[16]https://www.ibe.org.uk/resource/business-ethics-and-big-data.html
[17]https://imageware.io/passwordless-authentication/
[18]https://www.logonbox.com/content/eliminate-password-reset-tickets-to-increase-profits/
[19]https://www.itproportal.com/news/password-reuse-is-still-an-issue-for-businesses-everywhere/
[20]https://www.spiceworks.com/it-security/access-control/guest-article/the-power-of-passwordless-authentication-fortified-it-administration/

CONCLUSION

According to technology research and consulting firm Gartner, 60% of large-scale enterprises and 90% of small and medium-sized businesses will implement passwordless methods by the end of 2023[21]. There are certainly some challenges associated with moving to passwordless authentication, but the benefits far outweigh them. Improving user experience and cybersecurity posture, while reducing the cost ongoing of support are major benefits. Adopting passwordless authentication is the next logical step for businesses wanting to offer excellent user and employee experiences without compromising cybersecurity.

[21]https://www.gartner.com/smarterwithgartner/embrace-a-passwordless-approach-to-improve-security

CONTACT INFO

+61 8 8238 6500

sales@advance.net.au

www.advance.net.au