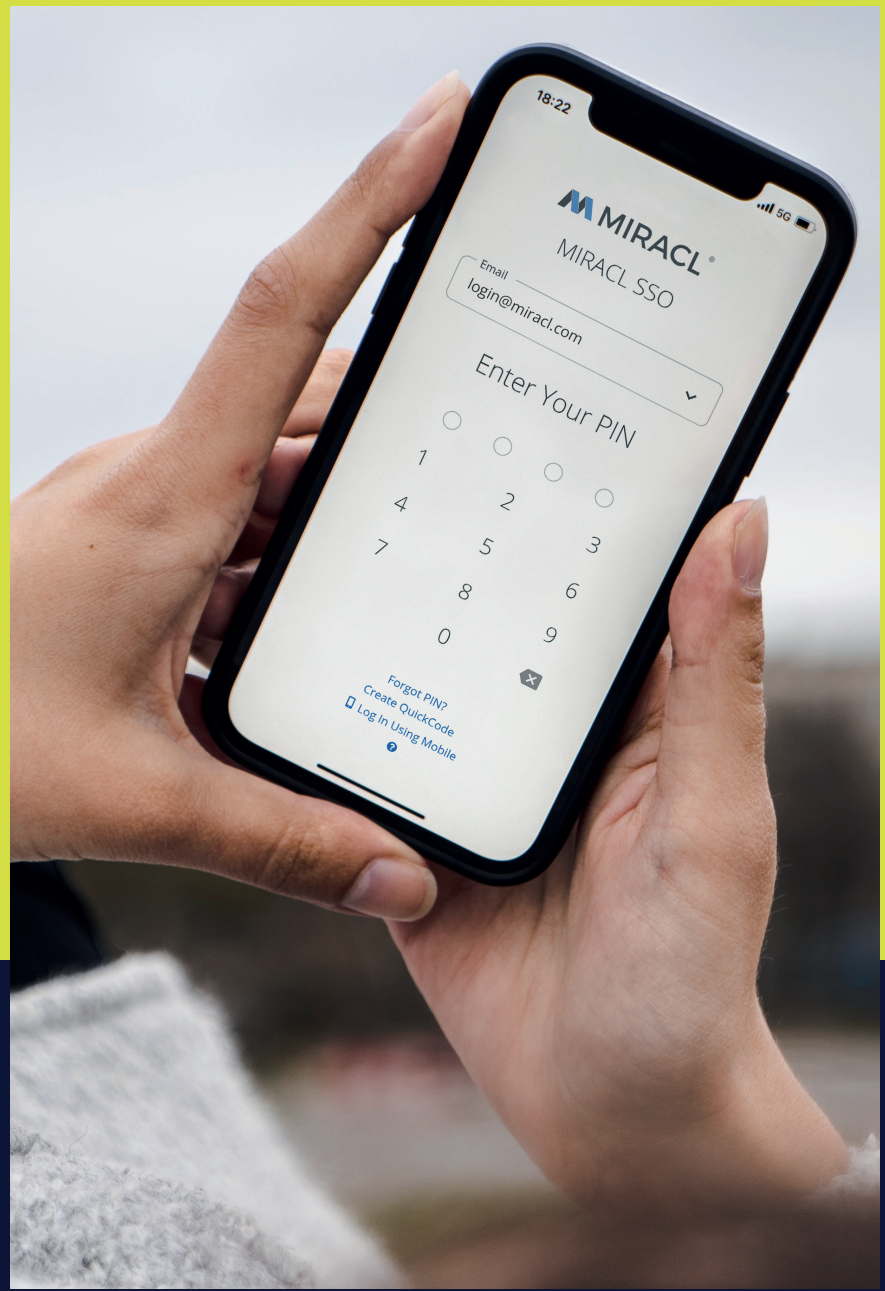
5 reasons to make your login your next big win



MIRACL®

About

It's a cliché to say that online business is changing fast. You know that already. So this ebook is about something that doesn't seem to change: a core component in almost every service that's strangely overlooked. It's about how this single process has a much wider impact than you might think. And how one quick, simple modification can dramatically improve your bottom line.

To call it a "key" ingredient sounds like another cliché, but in this case, it is exactly right. This ebook is about **authentication** – the keys we use everyday that keep us safe, unlock revenue, and open the door to great UX.

Photo by Markus Spiske on Unsplash

In a nutshell

1. Boost revenue
2. Great UX starts with authentication
3. Match your real-world security threats
4. It’s easy to switch
5. You’re spending too much

A step change hiding in plain sight

"The password helped us create a digital world built around computers. Now, let's create a world built around us."

– Professor Bill Buchanan, OBE, Phd, FBCS, PFHEA,CEng, BSc (Hons) and Professor of Applied Cryptography, Edinburgh Napier University.

Photo by NordWood Themes on Unsplash

Authentication is *the essential* process in our online lives. Whether logging in to email, modifying a shopping trolley, or approving a payment – almost everything we do means either accessing an account or creating a new one.

In more than 95% of cases, passwords are involved (source: Loginradius, 2020). First invented at the dawn of computing, passwords hold a unique distinction. Since those early days, UX in every other widely used process has improved beyond recognition, but **passwords have actually become harder to use**. That means more complicated to create, more difficult to remember and less secure.

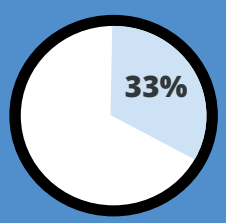
2FA (Two-factor Authentication) promised to bring security back to authentication. Yet most **MFA (Multi-factor Authentication)** systems only continue the strange evolution of the password: adding complexity to the user's journey, instead of taking it away. Most authentication today is clunkier than ever. You have to use two devices, configure an app, find a phone signal, and jump through unnecessary hoops.

That friction makes a real difference. Where UX matters most – in **retail, banking, gaming, and in leisure activities** – multi-step, multi-factor authentication and password problems have a direct, measurable impact on the bottom line.

That's why single-step MFA is much more than just the 'wow' factor of secure login in under two seconds. It's a step-change for your business, hiding in plain sight.

Most authentication today is clunkier than ever, and that friction makes a real difference.

Brits spend **22 hours** a year resetting their password.



33 percent of Brits have stated that changing passwords is the most annoying thing in their lives – even more annoying than losing their keys.

Source: https://www.silicon.co.uk/security/authentification/brits-spend-22-hours-per-year-changing-passwords-expressvpn-finds-487463

1

Boost revenue overnight

“I can’t believe the potential opportunity by simply improving the login experience. In retail, we care about customer relationships above all, and I know that logins are a friction point. Introducing one step multi-factor authentication is hugely valuable.”

– Lynsey Lambert, Vice President Product at Native Shoes and ex-Nike Retail Executive.

Photo by Luke Chesser on Unsplash

The industry standard for customer login success rates is exceptionally low, compared to the expectations placed on other essential provisions, such as system uptime. Depending on sector, authentication method and geography, **most businesses operate with the understanding that between 5% and 30% of logins will fail.**

What does that mean for those companies? When users cannot access their account, they do one of two things. Either they swallow their frustration and try again, perhaps by requesting a link to reset their password, or they give up and go elsewhere.

We wanted to understand how often the latter happens – how often people abandon a purchase – so in April 2022 we commissioned a YouGov survey of 2,000 UK adults to find out. A remarkable **25% said they leave a website and purchase from a competitor if they cannot remember their password.**

Now consider that some of the most common 2FA solutions are those that use SMS as a second-factor authentication, with a login failure rate ranging from 8% to as high as 20%. If one in four users (the 25% in the YouGov poll) react to that failure by abandoning their purchase, **companies are losing 2% to 5% of revenue minimum due to login failure**. Even a login success rate of 95% lets more than 1% of monthly revenue go to waste.

How can you recover those sales? The MIRACL solution, with its short PIN or biometric and superfast login, delivers a tried-and-tested authentication success rate of **99.6%**. That means next to no revenue is lost to login failure, and an immediate boost to your bottom line.

What is your login success rate?

Industry standards show average login success rate is 80%. MIRACL's average is 99.6%. Do you know what yours is?

2

UX starts with authentication

“With everyone from governments to global retailers, the common challenge is getting people to sign up. Replace the usability nightmares of passwords and MFA with a modern solution like MIRACL, and user accounts are going to become a whole lot more valuable.”

– UX specialist, Simon Richards, CEO at UX Agency Limited

Photo by Ed Hardie on Unsplash

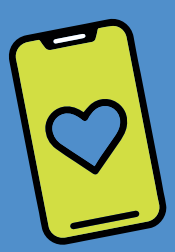
Logins have an outsize influence on your user experience. More than half of the UK consumers in our YouGov poll (56%) said they harbour negative feelings toward a brand or website after a poor login experience. Winning the trust of users is more and more essential in online retail. But in just a few seconds, a clunky authentication process can make that an uphill battle.

It's time to stop thinking of authentication as a necessary evil, and recognise that **poor UX has far-reaching consequences**. For example, the need for users to remember dozens of different, complex passwords is something many find so demanding that they resort to workarounds – reducing, rather than increasing security.

In one survey, almost all respondents (91%) said they understood the risk of password reuse, but 59% did it, regardless (source: iProov, 2020). The same survey revealed that **one in eight people use the same password for all sites and services**. With an estimated 24 billion stolen password credentials for sale on the dark web, (source: Digital Shadows, 2022) those reused passwords expose companies to significant risk of fraud.

Those who *do* use different passwords face the challenge of trying to remember them all. Many resort to resetting forgotten passwords – a frustrating, time-consuming process. As revealed in one study, half of Gen Z users (people born between 1997 and 2012) simply won't bother to reset a forgotten password. They just move on. (source: Transmit Security, 2022)

Great UX is essential for security and revenue. People should love their login, without resorting to workarounds. **Single-step MFA delivers great UX and great security**. With log in times of under two seconds and no need for a second device or complex password, it promises to dramatically improve security, revenue, and user relationships.



Poor UX has far-reaching consequences: from workarounds, to lost customers. How seamless is your authentication experience?

3

Match your real security threats

MIRACL is...

Compliant with:

- *GDPR*
- *PSD2*
- *New Jersey Gaming Regulation*
- *Ontario Gaming regulatory standards*

Resistant to all attacks:

- *Man-in-the-Middle*
- *Replay*
- *Credential Stuffing*
- *Password Spraying*
- *Phishing*

Photo by Philipp Katzenberger on Unsplash

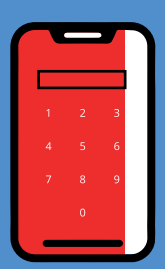
Compliance is often seen as the high-water mark for authorisation systems – the new end goal, when requirements are announced such as PSD2, or updates to the New Jersey gaming regulations. But because every company has to meet the same regulations in order to operate, **compliance is actually the *lowest* common denominator across a marketplace.** The minimum level of security, rather than the gold standard.

You could call it the **Compliance Paradox** – a trap that limits the ambition of authentication projects, and distracts from the real threats to a company's business.

It's the trap that caught out US gaming company DraftKings. The business was in total compliance with local New Jersey authorisation regulations, but it had not taken steps to prevent the specific problem of illegal "messenger betting", when local people act as proxies for gamblers outside the state.

After the scandal, the MFA processes that would have guarded against it were made compulsory in new regulation, but for DraftKings, the new standard came too late — the company received a $150,000 civil penalty in 2020.

Regulations only follow the curve. To stay ahead, businesses need to make a realistic assessment of the threats specific to their business, and take action.



Did you know that 80% of data breaches come from weak, compromised or reused passwords? Have you budgeted for data breaches or fines?

4

Switching over is easy

"MIRACL was able to integrate their single-step MFA codelessly, in just fifteen minutes – minimising disruption to services during the implementation phase, yet providing an added layer of IT security across the organisation."

– David Marshall, Head of ICT at Birmingham Women's and Children's NHS Foundation Trust

Photo by Karsten Winegeart on Unsplash

The success or failure of a digital transformation project can pivot on a single variable: duration. The longer the implementation, the less likely it is to meet the goals you set for it.

Older authentication systems can be slow to implement, creating compound problems for stakeholders: from software integration issues, to hardware.

Hardware security keys, or dongles, require logistical operations to roll out and scale. Even requiring users to have access to a device for one-time passwords (OTPs) can present a barrier to entry. And on the back-end, systems often run on servers which need to be configured and maintained.

Today, you can expect more.

SaaS authentication solutions eliminate the need for back-end maintenance and installation. Browser-based solutions mean users can authenticate through any device. Detailed SDKs make full integration straightforward.

And single-step MFA dramatically reduces user dependence on hardware, so no one has to rely on a dongle, or carry multiple devices.

In short, switching authentication systems is now simpler, speedier, and more likely to succeed than ever before.

Single-step MFA is as simple to setup as a password. At one UK health organisation, MIRACL integrated codelessly in just 15 minutes, minimising disruption to services.

5

You're spending too much

"When I first saw MIRACL, I was just fascinated by the technology. Without question: the user experience it provides makes it the one to go with. And on the commercial side, paying on a per-transaction basis is ideal for a startup looking to scale."

– Jim Lound, co-Founder at OBId

Photo by Karsten Winegeart on Unsplash

Most **multi-factor authentication** systems are much more expensive than they need to be.

Hardware keys are not just one of the most costly – and unsustainable – authentication systems to operate, thanks to their logistical requirements. They can also impose direct limits on growth, due to the need to distribute tokens.

Likewise, companies using one-time SMS passwords (OTP) have to pay for every SMS sent; costs often set by telecoms providers and intermediaries, exposing companies to third-party price fluctuations.

Behind many systems, one hidden cost is the installation, operation and maintenance of the servers required to run them. **Help desks are another: a staggering 20% to 70% of inquiries to company helpdesks are related to password resets.** According to Forrester, the average help desk labour cost of each of those resets comes in at around $70.

Compliance and security problems pose additional liabilities, whether in the form of fines or expenditure on remediation in the wake of breaches.

These costs need no longer apply. Hardware and back-end equipment can be replaced with SaaS browser-based solutions. Single-step MFA eliminates the need for SMS. **Successful login rates above 99% mean helpdesk costs can be cut or deployed elsewhere.** "Data light" solutions reduce exposure to compliance problems and security failures. And with per-use pricing, cost of ownership is kept in line with company activity.

$37

How much Twitter was paying per user per year for SMS OTPs

How much are you spending on authentication? Calculate your true cost of ownership: from SMS costs, to back-end maintenance and exposure to risk.

The change you can make today

The impact of great authentication can no longer be ignored.

Single-step MFA offers dramatic improvements to user experiences and immediate boosts to revenue.

Priced at one-tenth the cost of its competitors, with an unrivalled 99.6% login success rate, MIRACL is a dramatic upgrade from legacy solutions. One that sets authentication on a new path, simplifying, not complicating something we all have to do every day.

More reliable security. Direct cost savings.
And a painless setup.

A step change for your business — as easy to implement as it is to use.

Contact

Ready to see how your login can make you money?

Click here to schedule a Demo

Get in Touch
sales@miracl.com

Subscribe to our newsletter

For more information
miracl.com

Photo by Markus Spiske on Unsplash

The login you love

miracl.com

ISBN: [Ebook ISBN Number] ebook
Design by Mirador Labs Ltd
Edited by Margaret Sherer
Published by MIRACL Technologies ltd. www.miracl.com