When it comes to biometrics, are our bodies the best tool to protect privacy?

Using biometrics as a means of identification and authentication has been rapidly evolving. As consumers increase their use of digital channels and platforms, protecting their privacy and personal data is critical.

Temps de lecture : minute

20 October 2021

According to the latest study by *GetApp*, 47% of customers in the UK have willingly shared biometric data with a private company.

In March 2021, the *UK government* reported that 39% of businesses and 26% of charities experienced cyber security breaches or attacks in the past 12 months. The City of London Police, the UK national force for combating fraud, said it had received *3,916 reports of cybercrime* in just the first month of lockdown, equating to £2.9M in losses and reflecting an increase of almost 72% on the previous month.

Biometrics have often been seen as the ideal security tool. After all, fingerprints, voices, ear shape, retinas and gait are all unique to the individual. However, can these aspects of our physiology be trusted? In a world of deepfakes and regular headlines exposing how some biometrics can be beaten or confused, is biometrics the future of identity?

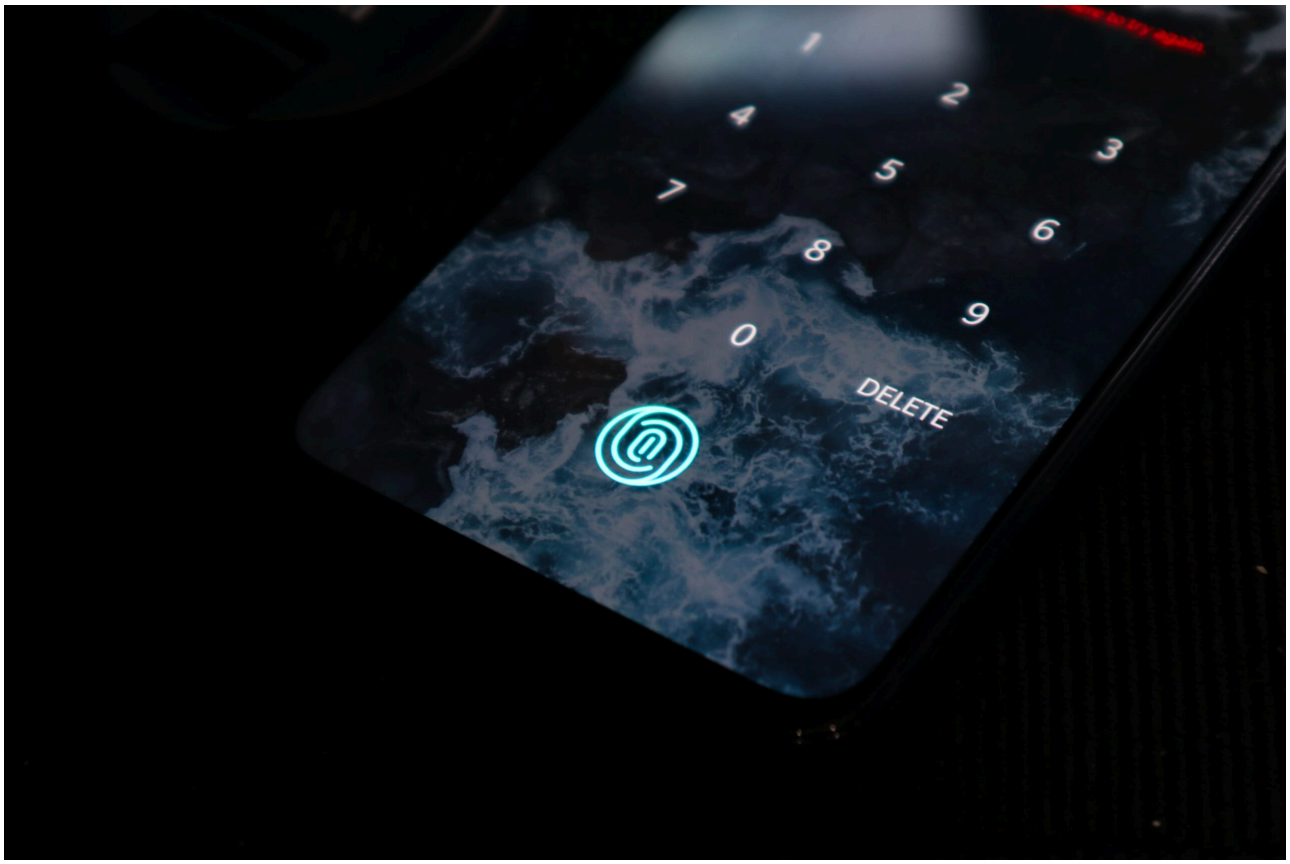
The power of the password

According to *LogMeIn*, 53% of consumers have not changed their

passwords in the last 12 months, with 42% worryingly stating that having an easy to remember password is more important to them than a secure password. The level of *risk awareness* is also high at 91%. However, 66% of respondents use the same or a variant of the same password.

With the average consumer having nearly 40 online accounts – many linked to their financial information – moving to a more convenient form of security such as biometrics seems the ideal solution to a growing cybersecurity threat.

The password has been the primary mechanism for accessing online accounts for decades. Passwords – when used with security front of mind – are effective. If a password is compromised, it can be easily replaced. This isn't possible if fingerprint or retinal scan-based access is breached: we can't replace our eyes just yet. But biometrics is also evolving to encompass behaviour biometrics that moves a step away from the unique physiological identifiers we all have to gather data about how we behave in any given scenario.



Businesses onboarding new customers need to be a fast, efficient, and cost-effective process. Passwords are highly attractive as they meet this trinity. Enterprises, though, have been expanding their use of multi-factor authentication to combat the rise of cybercrime. OTP (One-Time-Password) has been used by more online retailers to combat fraud. However, these identification methods do add a layer of friction that consumers with multiple accounts may find tiresome to manage.

Personal data is now massively valuable to businesses. How personal information is collected, stored, manipulated and shared is a hot topic of debate in the wake of data scandals such as Cambridge Analytica. Consumers are now acutely aware of the personal data they give in exchange for the services or goods they want to buy, but in many cases, how they approach the security of this information is often less than comprehensive.

Speaking to *Maddyness*, Armin Bauer, CTO and founder at IDnow, explained how mobile technology is leading to a biometric future: “Several European countries including Portugal, France, Germany, Switzerland and Austria are implementing changes to laws around NFC (Near Field Communication) technology to enable digital identification verification.

“France, for example, is leading the way with a new digital service for its citizens to allow them to access services on the government’s online services gateway, a system used by banks and other private sector companies as well as government agencies. Users only complete a single, straightforward application to access more than 500 government services instead of a separate onboarding process for each one.”

We are entering a biometric security future. However, biometrics is just one solution to the digital security puzzle.

The importance of online security

The awareness of biometric security has become more comprehensive thanks to the enhanced passports that the UK has issued for over a decade. In the broader commercial landscape, how businesses approach their digital security is tightening.

“Zero trust is becoming more popular a decade after it was first discussed,” said Neil Riva, principal product manager at JumpCloud. “The reason for this is that people realise they can’t make assumptions around security in the future, and they have to look at the whole process for access. Zero trust is also now becoming something that smaller businesses can adopt, rather than just being the preserve of large enterprises.”

Indeed, new research from *Illumio* concludes that zero trust as an approach to digital security is high on most companies' agendas, with 98% of UK business leaders and IT decision-makers either plan to or have already started implementing zero trust strategies at their organisations. Also, 60% of respondents stated the most significant benefit from their Zero Trust approach was feeling more confident they had secured their critical data and reduced their organisation's risk exposure (54%).

"This research makes one thing clear: UK business leaders and IT professionals know how important zero trust strategies are in making their organisations resilient, particularly as ransomware wreaks havoc across every industry," said Raghu Nandakumara, EMEA field CTO at Illumio.

Many of the biometric security systems in use today and those in development are using AI. However, Stuart Sharp, vice president of technical services at OneLogin, explains that AI is a double-edged sword: “AI powers many biometric technologies, such as facial recognition. But, on the other hand, AI can foil those same technologies, so we must be aware of the risks in depending on the power of AI for identification.

“Researchers recently developed a neural network capable of generating facial images that can simultaneously impersonate multiple identities.

“Further, according to a recent *study* from the European Parliamentary Research Service, the ostensibly reassuring performance of detection algorithms is not what it first seems. It found that because the performance of algorithms was often benchmarked against known and commonly used datasets, these algorithms were – in practice – good at detecting only a narrow subset of deepfakes. Furthermore, modifications, even small ones, would dramatically impact the final results generated by these systems.

Biometrics, then, is not a complete and reliable replacement for passwords. How businesses and governments manage the rising and diversifying cyberattacks will mean using tools such as AI.

More than skin deep

No discussion of personal security would not be complete without mentioning COVID-19. Personal data security has always been the foundation of online shopping. With the likelihood of digital e-passports becoming the norm, using some form of biometric security is inevitable.

With smartphones now ubiquitous, using these devices as the collection platform for biometric data is fast developing. Using what the digital payments industry has learnt about customer behaviour and how their services can be delivered via secure channels will form the basis of how we all prove we have been vaccinated.

“Voice is attractive in the post-pandemic world offering the promise of a truly touchless biometric and reducing the risk of surface transmission,” says Entrust's product marketing director for identity, Jennifer Markey.

“That said, I don't think it will become a dominant form of authentication. In general, a voice print is more easily faked and less secure than other biometrics. As well, voice technology is still evolving/emerging – think

about how many times Siri has played the wrong song or otherwise steered you wrong? Plus, much of our existing voice recognition technology was not architected with security as a primary use case. The other challenge is language: voice recognition is often optimised by language which limits its ability to address multilingual use cases."

As we enter the post-pandemic world, will we see a renaissance in personal digital security with biometrics at their foundation? Research from *Specops Software* reveals that more than three-quarters of Brits (78%) say they feel most comfortable using just the traditional password.

The token authentication method – where a small hardware device is used to authorise access to a network service – comes next, with 72% saying they feel safest using it. While fingerprint recognition is growing in popularity and many phone companies implementing this feature into their new smartphone devices, less than half (42%) of respondents said they feel truly comfortable using it.

And what of the future? The widespread adoption of multiple biometrics to secure personal information is on the far horizon. However, as consumers become more aware of the potential attacks they could sustain on their digital assets, a shift towards more secure identification methods will occur. Some of these methods will use biometrics.

Article by David Howell