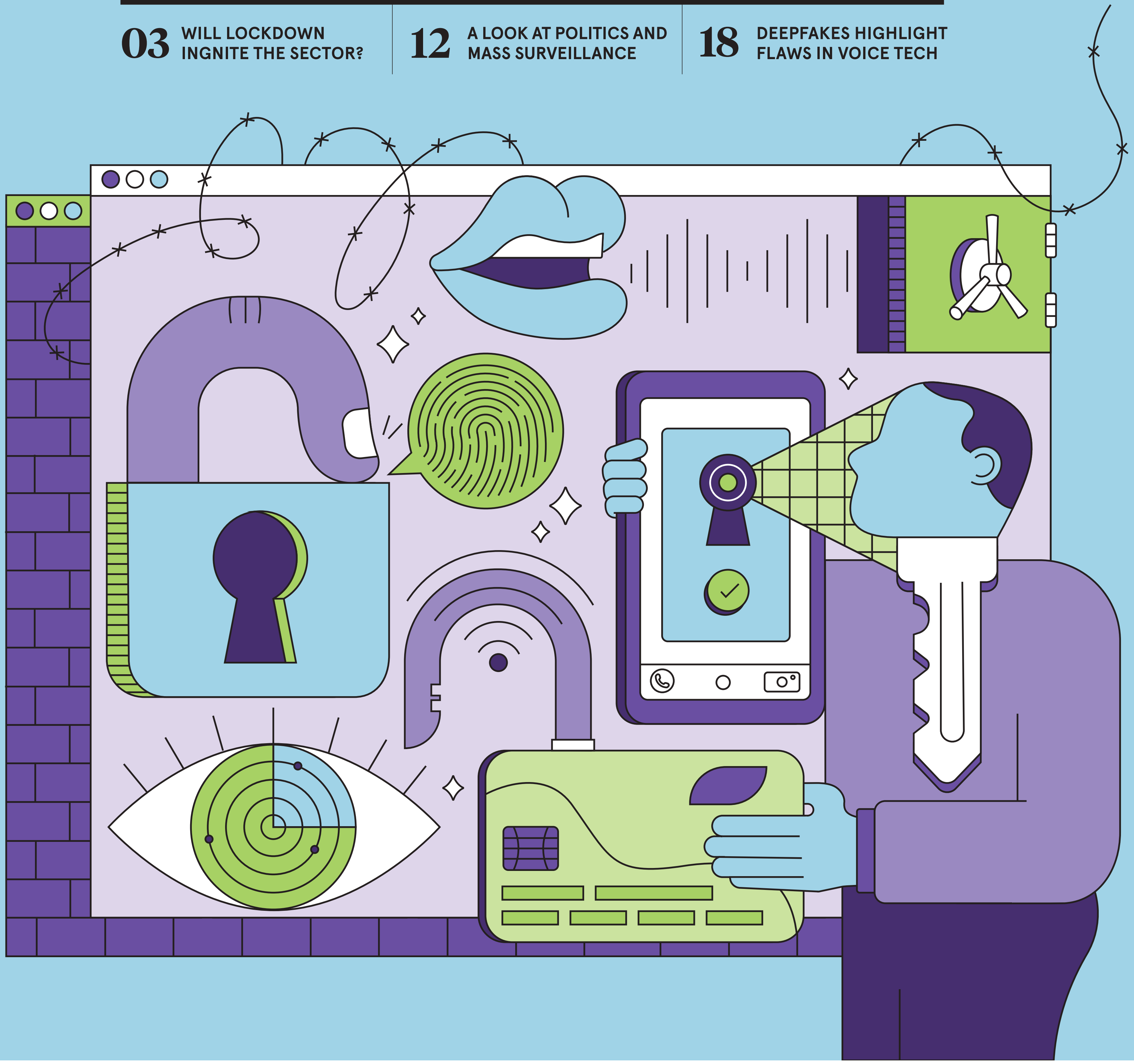
INDEPENDENT PUBLICATION BY

RACONTEUR

RACONTEUR.NET | #0662 | 05/05/2020

FUTURE OF AUTHENTICATION



TeleSign

The global leader in digital identity

Identity solutions for a digital world

Digital identity is the lifeblood of a dynamic ecosystem. TeleSign enables the world's largest brands to safely connect and engage with their customers throughout the globe. By delivering actionable user insights, TeleSign provides platforms with the ability to scale securely with verification, identity and communication solutions.

FUTURE OF AUTHENTICATION

Distributed in
THE TIMES

Published in association with
info security
STRATEGY | INSIGHT | TECHNOLOGY

Contributors

Nick Easen
Award-winning writer and broadcaster, he covers science, tech, economics and business, producing content for *BBC World News, CNN* and *Time*.

Christine Horton
Long-term contributor to specialist IT titles, including *Channel Pro* and *Microscope*, she writes about technology's impact on business.

Alexandra Leonards
Journalist, specialising in-depth features on a range of subjects, from current affairs and culture, to healthcare, technology and logistics.

Chris Stokel-Walker
Technology and culture journalist and author, his work has been published in *The New York Times, The Guardian* and *Wired*.

Marina Gerner
Award-winning arts, philosophy and finance writer, contributing to *The Economist's 1843, The Times Literary Supplement* and *Standpoint*.

Ed Jefferson
Journalist and creative technologist, his writing has been published in *The Guardian, New Statesman* and *CityMetric*.

Josh Sims
Journalist and editor contributing to a wide range of publications such as *Wallpaper, Spectator Life, Robb Report* and *Esquire*.

Peter Yeung
Award-winning journalist with a background in social anthropology, he has written for publications including *The Guardian, Wired* and *The BBC*.

raconteur reports

Publishing manager
Emma Ludditt

Associate editor
Peter Archer

Deputy editor
Francesca Cassidy

Managing editor
Benjamin Chiou

Digital content executive
Taryn Brickner

Head of production
Justyna O'Connell

Design
Sara Gelfgren
Kellie Jerrard
Harry Lewis-Irlam
Celina Lucey
Colm McDermott
Samuele Motta
Jack Woolrich

Art director
Joanna Bird

Design director
Tim Whitlock

Although this publication is funded through advertising and sponsorship, all editorial is without bias and sponsored features are clearly labelled. For an upcoming schedule, partnership inquiries or feedback, please call +44 (0)20 3877 3800 or email info@raconteur.net
Raconteur is a leading publisher of special-interest content and research. Its publications and articles cover a wide range of topics, including business, finance, sustainability, healthcare, lifestyle and technology. Raconteur special reports are published exclusively in *The Times* and *The Sunday Times* as well as online at raconteur.net
The information contained in this publication has been obtained from sources the Proprietors believe to be correct. However, no legal liability can be accepted for any errors. No part of this publication may be reproduced without the prior consent of the Publisher.

@raconteur /raconteur.net @raconteur_london

raconteur.net /authentication-2020

ADOPTION

A catalyst for change

Government-mandated home working has forced companies to reassess how they identify and onboard employees, and could prove to be a catalyst for strong growth in the authentication sector

Chris Stokel-Walker

As the coronavirus outbreak rewrites corporate rulebooks across the globe, businesses are starting to shift the way they work. Offices are being abandoned and more employees are working from home.

Ensuring continuity of business isn't simply a case of sending staff home with a work phone and laptop. Authentication methods that keep data secure and corporate networks safe are high on the list of all boardroom members, not just chief information security officers.

While business IT capabilities have been advancing at a pace, the COVID-19 pandemic is the catalyst for wider, faster change. It is set to be a tipping point for widespread adoption of strong authentication options.

"The world largely has the communications infrastructure in place to enable this unprecedented shift from in-office to remote work," says Andrew Shikiar, executive director of the FIDO Alliance, a non-profit consortium including big tech firms like Apple, Google, Facebook and Microsoft, which develops strong authentication methods for home working.

But there is a risk. "In this rush to enable remote work, it can be easy to overlook formal training and implementation of security best practices," he says. Proven authentication is important.

Network systems provider Cisco has helped businesses big and small move 17.5 million workers to safe home-working practices during the COVID-19 lockdown. Twelve million of those employees have used one of the company's multi-factor authentication (MFA) methods, while Cisco's Duo Security MFA product has seen double-digit percentage increases in the number of weekly sign-ups, according to John Maynard, Cisco's vice president of global security sales.

When employees largely accessed files and data from devices based in the office, it was easy to ensure they weren't compromised. Now, people are working from home, often on laptops and mobile phones that are also personal devices, and logging on to work networks through home broadband connections that could be compromised. So businesses have to adapt the way they work by providing employees with a method to prove it's them.

"There's a paradigm shift that has been happening in the security industry for some time, which is the concept of zero trust," says Maynard. Traditionally, anyone who was able to access a corporate network was given the keys to the castle because they must be trusted if they could get there. With home working, a rise in phishing attacks and a general increased awareness of cybersecurity issues, that's changing.

Sebastien Salom-Gomis/Getty Images

"In a zero-trust world, the default position for any user is they are untrusted until I can verify their identify and the health of their device," says Maynard.

The key question any number of authentication methods asks users is simple: "Are you really you?" Traditionally, we've relied on passwords to prove that.

"The first thing people think of is the longer your password, the better it's going to be," says Mike Johnstone, cybersecurity researcher at Western Australia's Edith Cowan University. But long passwords are unpopular.

The alternative is MFA to verify users. This can take the form of a text code sent to a user's mobile phone for them to enter once they've inserted their password or physical code generators that create single-use codes.

Google and Microsoft have authenticator apps, while biometrics such as fingerprints or facial recognition, are also useful authentication methods. "If having a single point or mechanism of authentication is a bad thing because it can be compromised in some way, having multiple means is generally better," says Johnstone.

That's something Thales Group, the international conglomerate that protects seven in ten credit and debit card transactions worldwide, knows too well. "We've never been in this situation before," says Howard Berg, senior vice president at Gemalto, a Thales company. "If you had something highly confidential to discuss, you'd arrange a meeting and see them face to face. Suddenly that's not available to us."

Thales employees have long used a smartcard similar to a credit card, inserted into a reader or directly into a PC, to authenticate users. The card cross-checks certificates with the device. If there's a match, the connection to Thales' internal network is made.

It's not just working from home, but also approving vital loans that now require alternative authentication methods. Hitachi Capital, one of the UK's leading business finance providers and a partner in disbursing the UK government's coronavirus business interruption loans scheme (CBILS), used legally to verify applicants for loans in person. Now that's not possible.

"As a partner in CBILS, we knew we needed a digital way to validate applicant identity for the vast majority of our business, which is handled indirectly via partners," says Jo Morris of Hitachi Capital Business Finance.

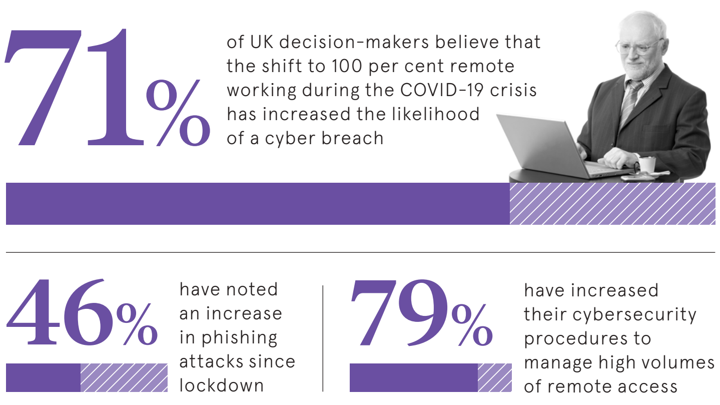
Hitachi has started using a two-step verification system, which cross-checks an identification document such as a passport with a "live" video selfie on a web-based platform provided by Nomidio, a biometric authentication service. The video prevents scamming the system. The approval process takes a minute.

"We're able to deliver a consistent ID check that's comparable to, if not even more convenient and secure, than our face-to-face process used pre-coronavirus," says Morris, who expects to use the Nomidio system after COVID-19.

She's not alone. "I think behaviour will change dramatically after this," says Berg. "We will probably have a different understanding of how we communicate when we're not face to face."

There'll be extra layers of authentication, whether using biometrics, codes or external devices like cards, more security built into the devices that we use to access communications systems and servers, and even other indicators, such as geolocation or behavioural biometrics, including the way we type or talk, to verify the person accessing systems is who they claim to be.

"We're suddenly in a situation where we're totally reliant on the world around us," says Berg, "and we're not able to do things physically as we always have." ●


71% of UK decision-makers believe that the shift to 100 per cent remote working during the COVID-19 crisis has increased the likelihood of a cyber breach

46% have noted an increase in phishing attacks since lockdown

79% have increased their cybersecurity procedures to manage high volumes of remote access

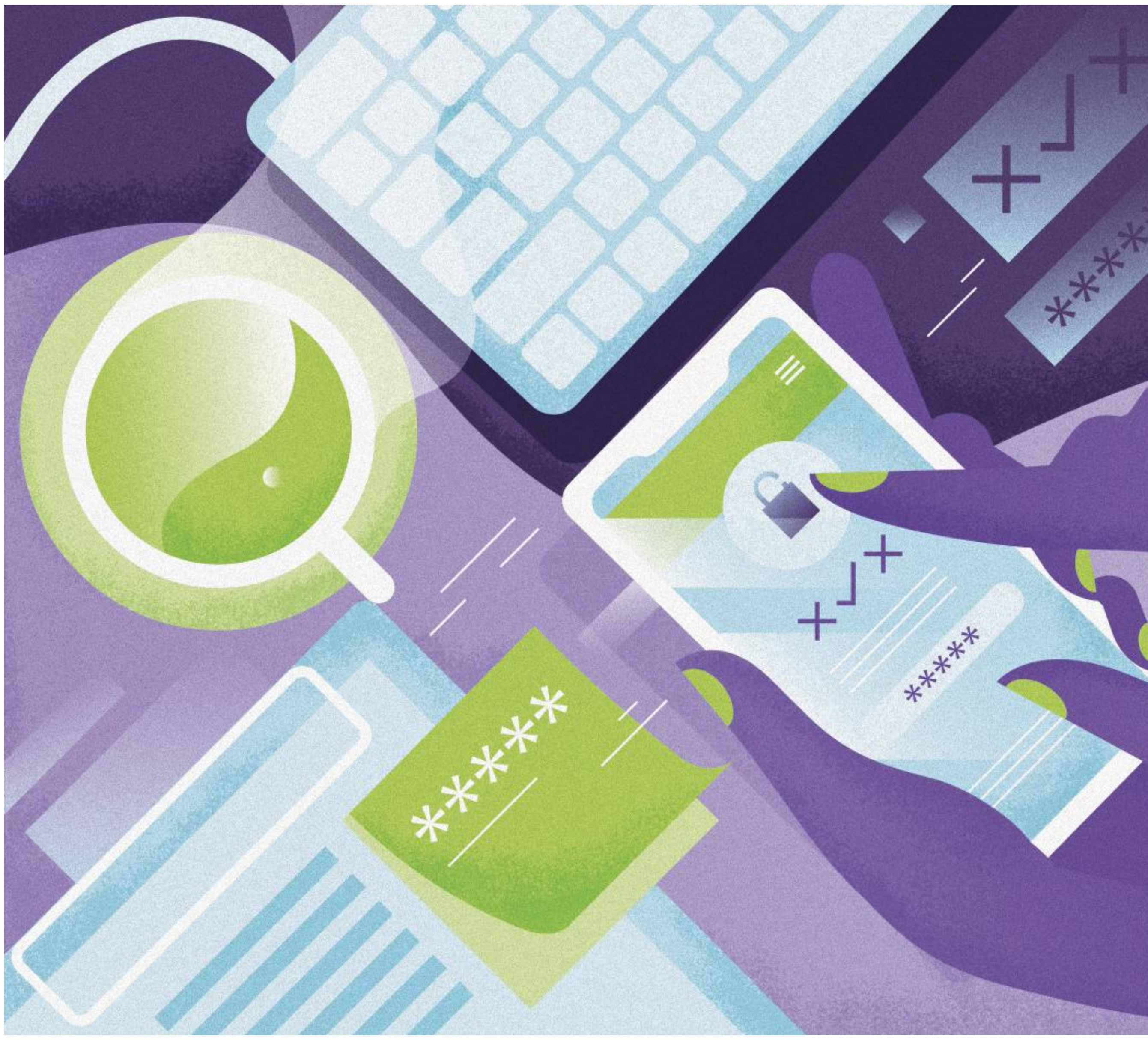
Centrify 2020

PASSWORDS

Why do passwords still exist?

Most cyber attacks and data breaches remain the result of weak password security. So, with a growing number of more secure alternatives now available, why are they still widely used?

Josh Sims



Using passwords to access our online lives is a commonplace experience and so are the attendant frustrations. Cybersecurity demands evermore complicated formulas: passwords might necessarily be of a minimum length, use a capital, number or special character. There is the regular insistence that a password be updated and not just to one slightly different or back to one you've used before.

"The good thing about passwords is they're easy to use and, if compromised, easy to replace," explains Mariam Nouh, researcher in cybersecurity at the University of Oxford. "There are no compatibility issues. You don't need extra hardware. And business likes them because their use can be implemented cost effectively. The problem though is they can be compromised in so many ways."

Certainly, while attempts at cybersecurity breaches may be evermore sophisticated, the fact is passwords butt up against human psychology or, more specifically, memory. There are only so many discrete passwords an individual can retain without the security no-no of writing them down, which is one reason for the rise of password vault software.

The result is, when possible, the use of familiar, emotionally significant phrases, which is to say utilising the same mechanisms behind how humans remember a lot of things. But the familiar makes it easier for hackers to crack the password.

According to a 2018 survey by password management company LastPass and Lab42, 59 per cent of respondents use the same password across multiple accounts. A majority of people would only go through the bother of updating their passwords if they were hacked; after all, they seem secure until that point. But then, according to a 2019 study by Verizon, 80 per cent of hacking-related security breaches are a result of weak or compromised credentials.

> "We're going to use passwords for some time because, from a security point of view, the whole system out there is just so complex

When LinkedIn suffered a data breach in 2012 and some 117 million passwords were compromised, many were revealed to be rather obvious. Among those used hundreds of thousands of times were "123456", "linkedin" and "password".

"There's a lot of dissonance between how we know we should use passwords and how we actually do," says Rachael Stockton, senior director of product at LogMeIn, makers of LastPass. And it's not just a matter of memory. "A lot of our customers are just after simplicity, less time-wasting and more productivity. And we're going to need more simplicity [in our password management] because the number of accounts we each use on the internet is only going to increase," she says.

That most of us don't make much effort with our passwords isn't just our fault. Arguably, security software design has failed to take human psychology into consideration.

"The industry has not done well in educating consumers how to use passwords," concedes Rolf Lindermann, vice president of product at Nok Nok Labs, an authentication software vendor. "The result is this trade-off between security and convenience. That's the dilemma."

And especially given the vast majority of websites still use passwords. It's estimated there are now some 300 billion active passwords. Even Fernando Corbato, the man who pioneered the use of the password online, has described the situation as a "kind of nightmare".

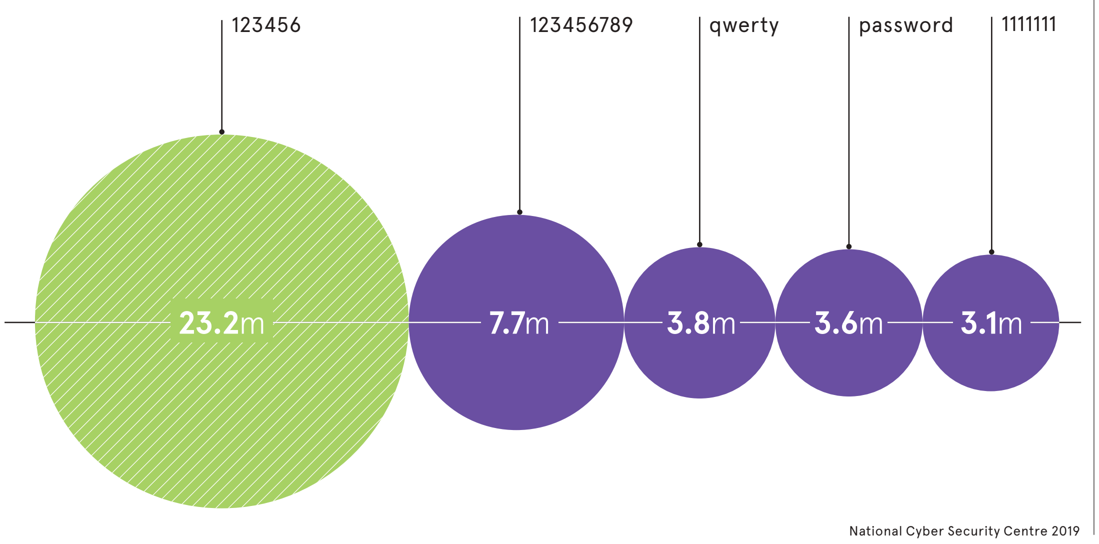
There have been new kinds of passwords proposed. Because people recognise pictures better than they remember words, so-called graphical passwords request users click certain points on an image in a certain order. The number of possible points essentially makes each user's sequence unguessable. The efficacy of this approach is still being worked out.

But the likes of George Waller, co-founder of StrikeForce Technologies, a US startup with a number of patented cybersecurity inventions under its belt, argues the problem isn't with passwords per se. Although he points out that most online businesses typically want to offer consumers the path of least resistance to gain access to their sites. The problem is with passwords' delivery to servers down the line.

"Ultimately, it's not really a matter of whether we use passwords or not, or whether or not you enforce stricter policies on their use. It doesn't matter so much what you

MOST USED PASSWORDS

Analysis of breached accounts worldwide



National Cyber Security Centre 2019

type in because there typically isn't encryption at the key-stroke level and data is in transit [and so vulnerable] from the time you start typing your password," he says. "We're going to use passwords for quite some time because, from a security point of view, the whole system out there is just so complex."

So does the password have any future, especially given the advent of the internet of things, which only looks like making cybersecurity breaches more widespread? "Passwords won't go away completely, but I think we have to expect more multi-factor authentication, though that still needs to be convenient to use, while offering a sensible level of security to carry the public with it," says Oxford's Nouh.

This layered security approach is unlikely to come in the form of biometrics, which are themselves not completely secure and, when stolen, irreplaceable, unlike a password. Or at least not just biometrics. What's needed, Lindermann contends, is however secure sites are accessed, we're tied to a device that can be used to identify us. And this is a device most of us already carry and increasingly use to access the internet anyway: our smartphones.

We're increasingly used to receiving confirmation text messages when working through security. But now such devices also operate their own fingerprint or facial recognition systems. Features limited to high-end, expensive phones just five years ago are increasingly commonplace and accessibly priced.

59%

of people use the same password across multiple accounts

LastPass/Lab42 2018

80%

of hacking-related security breaches are a result of weak or compromised credentials

Verizon 2010

Since Microsoft launched its Windows 10 operating system last year, such password-free authentication is starting to come to desktops too. Device geolocation – if users are willing to share such information – is potentially another added layer of security.

Indeed, in a sense this more efficient device-led proposal is akin to the way in which an ATM requires both PIN number and the physical bank card. Or the way in which Estonia, for example, has developed its e-Identity system, which provides all citizens with a chip-and-pin e-card designed to authenticate an individual's digital identity.

Lindermann says: "It's a matter of leveraging these devices in the right way and in a consistent way; one that allows users to chose the modality – they can still use a PIN if they're not comfortable with trusting their biometrics [to a third party] – but which ties their identity to the specific device, a capability that can be off-loaded to devices we don't own on the rare occasions that's needed. It works because people want a much easier engagement with business that have secured sites and the ease of use is better for business too."

Andrew Shikiar agrees. He's the executive director of the FIDO Alliance, a consortium of tech security companies pushing for the creation of an industry standard to address security interoperability between devices and so far supported by big guns the likes of American Express, Amazon and Google.

"Passwords are the tip of the spear of the data-breach problem," says Shikiar. "But the fundamental problem is the [online security] architecture itself. Using devices would not only give a better user experience – people are already used to unlocking their phones using biometrics – but it would get rid of scaleable cyber attacks. It would necessitate a behavioural change, but we have to break our dependence on passwords."

He's betting on that happening soon. He reckons the majority of mainstream consumer services online will have a password-free means of accessing them within five years. ●

Commercial feature

Blunt truth about authentication: it's not just about security

Customer-centric businesses prioritise a frictionless user experience as well as protection of consumers from fraud

The COVID-19 pandemic has triggered an explosion in digital fraud. The UK's national fraud reporting centre has received thousands of reports of phishing attempts that exploit people's fears of coronavirus.

The health crisis has illuminated a prevailing misconception that authentication is all about security. Wiser businesses, however, know security mustn't jeopardise customer experience. And delivering it in a customer-centric, frictionless way necessitates smart onboarding and authentication.

Needless to say, this isn't easy. Authentication is not a single event anymore; it's a journey that flows from customer onboarding to mobile, web and contact centre authentication, to account recovery. Using multiple solutions for each step makes seamlessness all but impossible.

"The truth is most identity platforms are very secure, but some unintentionally add unnecessary friction to the user experience," says Clive Bourke, president, Europe, Middle East, Africa and Asia-Pacific, at Daon, which develops and deploys customer onboarding and authentication solutions.

"When a company puts out a request for a new customer identity solution, too often the specifications revolve more around secure authentication and less customer engagement or how the customers are registered in the first place."

Companies will benefit from a single platform that connects all channels and stages of their customer identity life cycle. Daon has pioneered methods for securely and conveniently combining biometric and identity capabilities across multiple channels. Its *IdentityX*® platform orchestrates the creation, authentication and recovery of a user's identity and allows businesses to conduct transactions seamlessly with any end-customer.

With this approach, security and ease of use need no longer be opposing priorities. US financial services firm USAA has reported zero evidence of mobile channel fraud while simultaneously achieving the highest net promoter score in banking for the tenth consecutive year.

Atom bank has personalised and streamlined onboarding and authentication for its customers, registering their face, voice and a PIN when onboarding them and then using the biometrics to authenticate them easily later.

"Prioritising security and customer service is fundamental," says Rana Bhattacharya, chief technology officer at Atom bank, the UK's first bank built exclusively for mobile and the number-one rated UK bank on Trustpilot.

"We exist to create better customer outcomes and want to take the worry, frustration and pain of existing processes away for our customers by offering them the best possible experience when using our products. We're constantly listening to our customers' feedback, which is invaluable to us and we use this feedback to make things better for them."

Sumitomo Mitsui Financial Group (SMFG) is monetising these services through Polarify, a joint venture with SMFG, Daon and NTT Data that provides Electronic Know-Your-Customer (e-KYC), or onboarding, and authentication as a service in the Japanese market.

"The speed with which the digital market is changing in Japan is phenomenal and users are demanding frictionless and security in equal measure," says Polarify chief executive Tomohiro Wada. "We now have dozens of customers doing cross-channel onboarding and authentication, which proves the demand for solving this problem."

Daon advises companies to start with digital onboarding, allowing customers to open an account on a mobile app or web browser, anytime, anywhere. This can be secured by three-dimensional facial biometrics that detect fraudulent presentation attacks, and the user-friendly process completes in minutes.

Next, banks should solve authentication issues across all channels, including the contact centre, which is often the biggest challenge. By bringing voice biometrics and other factors to their customers, they can prevent fraud losses, reduce their average call time by 25 to 45 seconds, contain more calls within interactive voice response and deliver markedly better customer experiences, in addition to better security.

"The smart companies understand it's about security and a frictionless experience for their customers," says Daon's Bourke. "Now they are focusing on orchestrating a consistent onboarding and authentication capability that can be reused across brands to deliver seamless cross-channel user journeys to their customers."

BETTER CUSTOMER ENGAGEMENT

62%

of respondents reported 'high' to 'very high' increases in customer satisfaction benefits as a result of deploying biometrics

INCREASE TO NET PROMOTER SCORE

45%

reported a 'very high' increase in their Net Promoter Score as a result of deploying biometrics

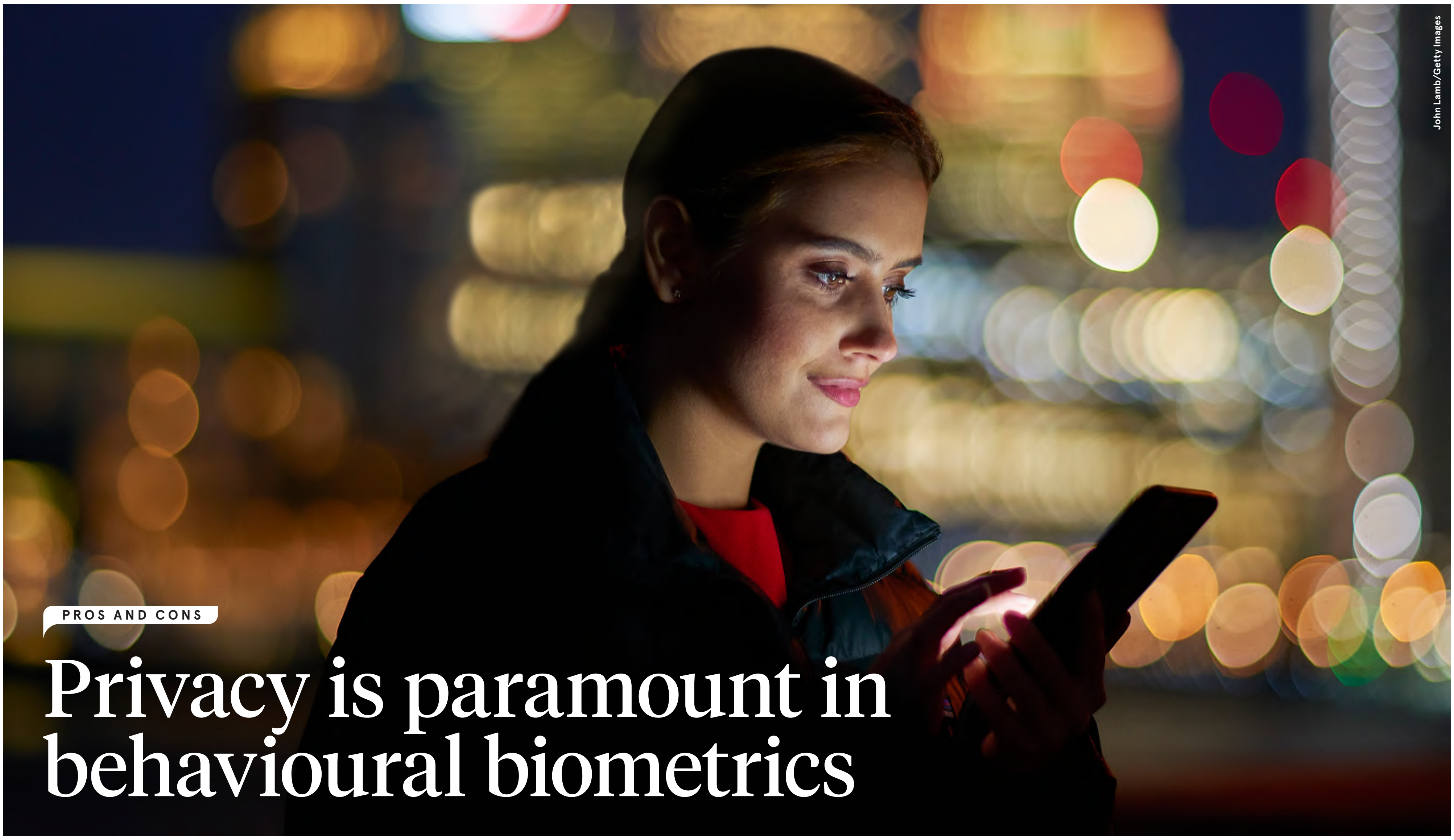
$10m

cost savings from using a well-orchestrated cross-channel onboarding and authentication platform

Goode Intelligence Survey of Global Financial Services Organisations

For more information please visit www.daon.com

Daon®



John Lamb/Getty Images

PROS AND CONS

Privacy is paramount in behavioural biometrics

Behavioural biometrics offer an additional layer of security to identify customers, but come with a host of privacy and ethical concerns that must be addressed. Experts debate the pros and cons

Marina Gerner

Pros

In the wake of the Sony hack and Cambridge Analytica scandal, concerns around online data have engaged public discourse. When it comes to financial institutions, new ways of handling their customers' data, and verifying who they are, have been introduced at a rapid pace.

In a bid to authenticate customers more efficiently, banks are turning to new metrics. They are moving from knowledge-based entries such as passwords and security questions to biometrics like our faces and fingerprints. But so-called behavioural biometrics are increasingly used to analyse how tightly we grasp our phone, how swiftly we swipe and how evenly we walk.

So, if you're not typing as fast as you normally would, the system might fail to authenticate you. One advantage of these metrics is that it's supposedly almost impossible to steal or replicate.

"Behavioural biometrics can be collected unobtrusively and multiple modalities can be collected at the same time, providing for better authentication and making it more difficult to spoof them," says Dr Roman V. Yampolskiy, associate professor of computer science and engineering at the University of Louisville.

In addition to efficiency, behavioural biometrics are a way for financial institutions to respond to ever-increasing regulatory requirements for multi-factor authentication. Instead of requiring customers to enter multiple passwords and codes, which most people find fatiguing, biometrics offer a way of passively authenticating users without them having to make an effort.

Once financial companies have behavioural biometric data, its application could go beyond authentication.

"There has been some data that suggests such behavioural biometrics can be used not just to identify the individual, but to provide some indication of aspects of that person's personality profile," says Greg Davies, head of behavioural finance at Oxford Risk. "If so, these techniques could also be used to supplement existing client profiling processes, helping to establish more personalised and targeted communications and client engagement."

But behavioural biometrics don't just happen with your conscious input, they happen without most people's knowledge too. They're run behind the scenes. While behavioural biometrics hold huge potential for improving the security and usability of authentication processes, let's not overlook the major drawbacks to this method.

Customers will have given their consent for data collection, but terms and conditions can be opaque and confusing when data is at stake.

> "
> **If biometrics are not just telling me who you are, but also how best to communicate and sell to you, then this has consequences**

Cons

Let's consider the other side of the story. Given that financial institutions or technology companies don't typically share the extent to which they monitor their clients' behaviour, instead forging ahead with new metrics and analytics, privacy and transparency can suffer. It's the crux of any data collection method.

With hacking and fraud on the rise, financial institutions will have to work hard to protect their customers' data in the process of their identity authentication. As Yampolskiy at the University of Louisville notes: "Behaviour is strongly related to cognitive function and so collecting behavioural observations in many cases means privacy violations, which may uncover undesirable aspects for public disclosure information, such as illnesses."

Another issue with biometric data collection is that it can be biased. If most of the systems have been trained to recognise and measure the activities of white men, for example, they won't be as good at analysing the biometrics of women and ethnic minorities. This could result in false positives or declined logins.

Davies at Oxford Risk agrees there are a number of reasons to be cautious about behavioural biometrics. He says there would need to be "a lot of empirical validation to ensure these techniques are establishing something valid and stable, and reliable about the individual". This also means excluding the possibility such methodologies don't provide unreliable results if they were measured at specific times, for example, when the person was stressed or exercising.

"If biometrics are not just telling me who you are, but also how best to communicate and sell to you, then this has large consequences for the use of some data," Davies adds.

Customers expect more accuracy from brands' online communication, but too much targeting can be creepy. So what can be done to address these downsides and ensure customer data is protected?

Yampolskiy points out that algorithmic techniques for obfuscation of collected data, such as hashing, which is a way of increasing security during the process of message transmission, may help reduce some of the privacy concerns.

"I'd say the use of such profiling needs to be very careful and transparent," says Davies, adding it's likely behavioural biometrics will be used beyond the realms of authentication. He says there is less danger in using such profiling to improve client engagement and communication, but a fairly high risk if it was used to guide people with long-term investment advice.

"Being very clear about where each measure is used is vital, as is ensuring all use is made transparent to users and regulators," Davies concludes. ●

Human versus machine: which provides the highest assurance levels?

During the coronavirus lockdown, as millions are working and shopping from home, verifying people digitally with biometrics and checks by experts has never been more vital

The financial services sector faces a critical juncture. With quarantines, social distancing and stay-at-home orders all in place, digital tools are among the only means by which consumers can communicate with institutions around the globe. The coronavirus pandemic has therefore put trust in remote digital onboarding centre stage.

It's not just banking. Government benefits, health services, online education, dating companies and gaming are just some of the sectors witnessing a huge surge in demand for digital know-your-customer services. This is expanding the use of digital authentication. The outbreak is also proving fertile ground for fraudsters exploiting the global rise in onboarding.

"Trust is paramount. You need to trust a system that's going to take physical identity documents and live images of real people and turn them into digital identities. Anyone who tells you they can fully automate this process without some degree of fraud risk is not telling the truth," explains Joe Bloemendaal, head of strategy at Mitek Systems, a global leader in digital identity verification.

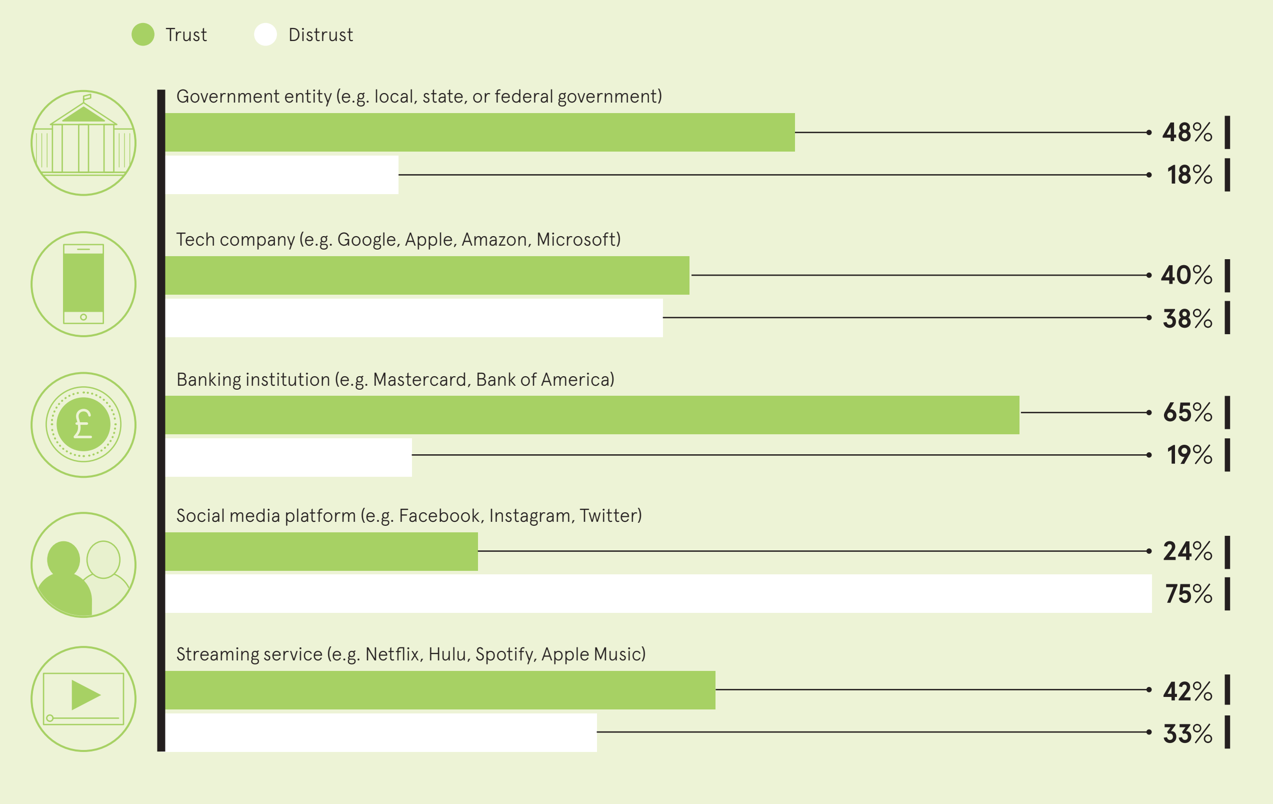
"Even in 2020, as economies digitise fast, most forms of ID globally are stuck in the analogue world. There is no comprehensive, interoperable digital identity that exists anywhere. Fraudsters are hot on our heels creating fake IDs and we estimate that about 20 per cent of the techniques they deploy each year are new. You cannot account for all types of ingenious fraud in an automated system."

The science behind digital authentication has become more complex, vigorous and automated than at any point in history. Machine-learning algorithms can digest multiple security features in a passport or driving licence and know whether it's fake. This is then combined with the ubiquity of smartphones to verify the consumer using a selfie and liveness detection, which recognises whether a person is real.

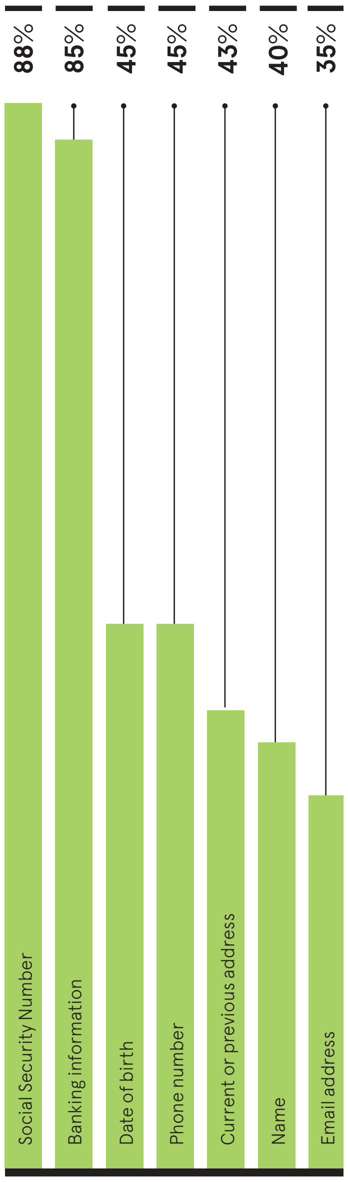
"Right now, computers may be better at facial recognition, but an experienced agent is still better at spotting fraud in some forms of paper ID. Therefore, we still need human experts to assist in digital onboarding. Having been around for over 36 years, we have a huge amount of experience in this area. We've always had experts and they know what the latest fraudulent activity looks like," says Bloemendaal.

> We all need a system we can trust to authenticate the massive shift to online services

CONSUMERS' LEVEL OF TRUST WITH THE PROTECTION OF THEIR DATA



CONSUMERS' TOP CONCERNS FOR THE SECURITY OF PERSONALLY IDENTIFIABLE INFORMATION (PII)



"It's true that fully automated systems can be faster and sufficient for many requirements. Artificial intelligence-powered technology can recognise a valid ID as genuine and match the ID photo with a selfie using biometric facial comparison. But while algorithms are powerful, they are not perfect. There will be exceptions that the technology has not yet been trained to recognise. This is where agent-assisted solutions come into their own."

Trust matters most in the digital world and onboarding process. Customers value signals that their online identities aren't just automatically being processed, but carefully considered. This is known as positive friction and a small amount of it is seen as a good thing.

In a survey by Experian, 66 per cent of people polled said they like security protocols when they interact online because it makes them feel protected. In another poll, 86 per cent of consumers say they value security over convenience in digital channels.

"Digital onboarding is analogous to flying an Airbus A380. Most functions of the flight are now automated and digitalised. But no passenger actually wants to fly with a computer in charge. The pilot gives them assurance and takes control at crucial times. This is no different to digital onboarding," says Bloemendaal.

"This is how we view the process. You still need humans to reach necessary levels of assurance. And taking a little extra time to digitally onboard someone is a good balance between positive friction, user friendliness and building trust. Automation, machine-learning algorithms, even artificial intelligence are all there to empower humans and vice versa. It's not human or machine, it's about using the best of both."

This also allows machines to learn from experts. Machines don't teach themselves. Capturing the latest fraudulent ID and feeding these into powerful analytical systems so computers can spot fake documents is how the machine's abilities are continually improved.

"We've had a lot of inquiries with the COVID-19 outbreak. We all need a system we can trust to authenticate the massive shift to online services. Verifying people digitally has never been more vital, especially in an age when phishing and synthetic identities are surging," says Bloemendaal.

"These are crucial times for the biometric industry. It is essential to get digital onboarding right in the rush to authenticate and verify many more people. Their lives depend on it, whether it involves new interactions with banks or governments."

An example of where human and machine are working together is the fight against synthetic identity fraud. This occurs when criminals combine real and false information into new, bogus IDs to commit financial crime. Big in North America, it is now spreading across Europe. There are no audit trails and this type of fraud allows criminals to build up a credit score, create new bank accounts and then exploit the financial system.

"A very robust check of an ID document using the right identity verification solution can help in the fight against this crime. Combining this with a mobile phone selfie, a liveness test and an expert eye, which then counter checks all elements of a person's identity, provides a robust system," says Bloemendaal.

The future certainly looks bright for biometrics. Using the best of human and machine, digital authentication and verification are now merging and also reaching new audiences. "These are exciting times. Mitek Systems is at the forefront. You will soon see biometrics used to verify much larger bank payments and authenticating an older generation into the digital world," Bloemendaal concludes.

Mitek Systems is a Nasdaq-listed company, which has worked with 7,000 organisations around the world, servicing more than 80 million users.

For more information please visit miteksystems.com

Mitek

CYBERSECURITY

Five key ways to strengthen your enterprise security

As cyber attacks increase in frequency and complexity, organisations are investing in security solutions that go beyond passwords. With 60 per cent of hacking incidents now involving the use of stolen credentials, here are five ways companies can use authentication to provide additional layers of protection

Christine Horton

1 Multi-factor authentication

Multi-factor authentication, or MFA, requires you to have more than just your username and password to log in to an account. After you enter your username and password it also requires a second piece of information, such as biometric authentication of your fingerprint, that can't be easily spoofed by an attacker.

Other methods include receiving a SMS one-time code on your smartphone that must be entered alongside the username and password or the use of a hardware factor, such as Google's Titan Security Key.

The good news is there is already broad awareness and usage of MFA. According to LogMeIn's 2020 *Psychology of Passwords* report, 54 per cent of surveyed organisations worldwide say they use MFA for their personal accounts and 37 per cent use it at work.

While it dramatically increases business security, one downside is that MFA requires users have a smartphone, or biometric reader or card-reading device at hand. This desire to reduce user friction is one reason why some digital service providers still rely on inherently unsecure passwords.

2 Biometric authentication

A type of MFA, fingerprint, iris, face and voice recognition are already found on most smartphones, tablets and computers. The use of biometrics to ensure business security is also gaining popularity, with LogMeIn's research reporting 65 per cent of organisations trust fingerprint or facial recognition more than traditional text passwords.

Indeed, HSBC UK recently announced that its VoiceID voice biometrics system prevented almost £400 million of customers' money from falling into the hands of telephone fraudsters last year, with the rate of attempted fraud doubling, year on year.

However, Andrew Shikiar, executive director of the FIDO Alliance, which develops and promotes authentication standards, says breaches such as that against the Biostar 2 platform in August 2019 demonstrate the risks associated with mismanagement of user biometrics.

"While it's certainly inconvenient and damaging to have your password stolen, the impact of a stolen biometric is far worse as they inherently cannot be changed," he says.

3 Adaptive/risk-based authentication

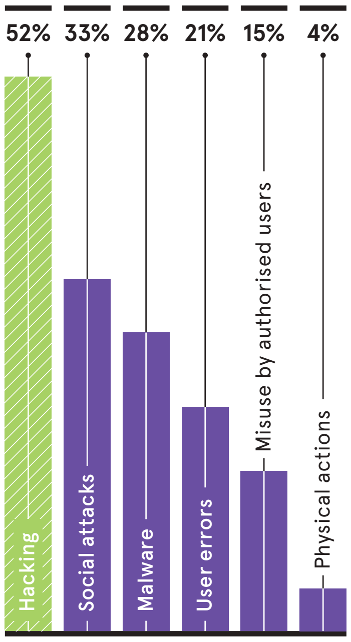
There are a host of security technologies that work unseen to validate the legitimacy of the person requesting digital access.

One such method is the use of secure smartphone and tablet apps that have built-in security controls, such as a biometric scanner. Other approaches include examining the login device to check for the presence of a secure digital token, as well as comparing each login with previous behaviour, which can include the IP address used and geographic location.

Glenn Carstens-Peters /Unsplash

COMMON TACTICS USED IN CYBERATTACKS

Analysis of 41,686 security incidents in 2019, of which 2,013 were confirmed data breaches; percentage of breaches that included the following tactics



Verizon 2019

These systems tend to use risk-scoring so if something is statistically suspicious, it may prompt for additional checks such as MFA or asking a security question.

Phil Allen, vice president, Europe, Middle East and Africa, at security software firm Ping Identity, notes that while risk-based authentication, sometimes known as adaptive authentication, is generally used alongside passwords and MFA, they are good at spotting more subtle attacks.

"Banks use these methods to spot fraudulent credit card payments; for example, buying a large TV in a shop in Edinburgh when the card was used two hours previously at a petrol station in Birmingham would almost certainly trigger an additional verification check," he explains.

4 Continual/zero-trust authentication

One of the biggest issues for organisations is most business security architecture assumes once a user is granted access to the corporate network, they are then trusted and can gain access to applications and data as needed.

However, according to Verizon's *2019 Data Breach Investigations Report*, a third of all cybersecurity breaches have an insider element that includes disgruntled employees or user error. Also, a legitimate user who has gained secure access through the perimeter may be an unwitting Trojan Horse for a hacker who has breached their access device and is piggybacking into the corporate local area network, or LAN.

As such, more organisations are moving to a zero-trust model where users are authenticated continually for every application and data access they require. This includes behavioural analytics and geolocation analysis to help spot suspicious behaviour.

"Once instigated, this makes it much easier to add new applications, adapt policies for new regulatory or security requirements and, best of all in the current situation, it is particularly well suited to securing access for remote working," says Allen at Ping Identity.

5 Public key infrastructure

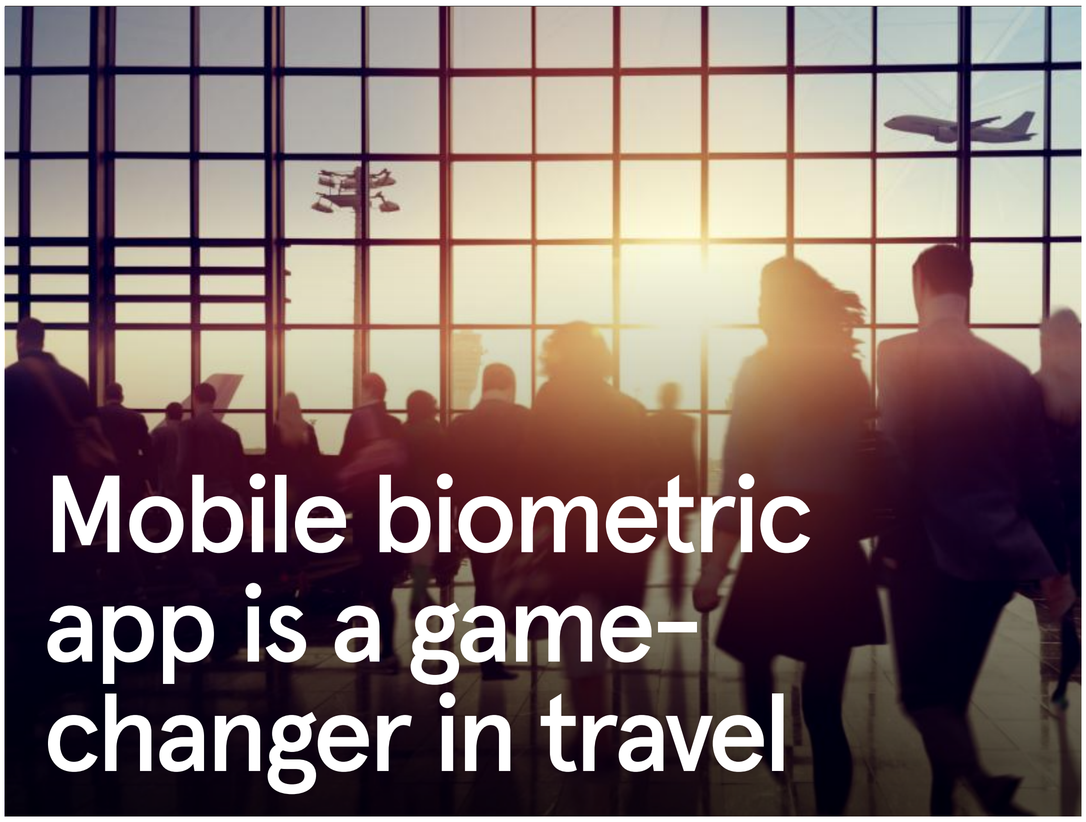
First developed more than 40 years ago, public key infrastructure, or PKI, is one of the longest-standing methods of authentication. It involves the use of two keys, one private and the other public. You use these to encrypt messages that can only be deciphered by applying the other key. Authentication is achieved by using digital certificates, which are issued by a trusted third party known as a certificate authority.

"PKI authentication is far easier in use-cases where it is onerous for the person to type a password and supply a second factor," says Mike Hathaway, chief technology officer at Ascertia, which develops digital-signing solutions.

PKI is also a best-practice method of authenticating devices and applications without the need for an administrator entering a password.

However, while PKI is well established and trusted by organisations for their business security, it can be more resource-intensive to manage and is regarded as more costly than other authentication methods. ●

Commercial feature



Mobile biometric app is a game-changer in travel

With social distancing likely to continue for months, a mobile biometric app could keep passengers passing safely through airports

With social distancing likely to continue for months, a mobile biometric app could keep passengers passing safely through airports.

Even before the challenging times the air transport industry is now facing, many airports were already operating at full capacity. When the global economy ramps up after the coronavirus outbreak, passenger numbers are likely to climb again. The current respite and social distancing that will be needed should be a time when airports review their passenger flows.

"The ultimate goal for any airport is to make the experience as hassle-free as possible, balancing the security and the seamless movement of travellers," explains Matthias Karl Koehler, vice president at Mühlbauer, a global leader in biometric identification and border management systems.

"Managing passengers in a smart and reliable way, with little disturbance, easy ID and boarding checks, is crucial. Currently, there are bottlenecks at passport control and at checkpoints, so with COVID-19 still looming large, people in close proximity could be an issue."

> “In the current situation, it would be much better if data reading devices were mobile, creating better traveller flow and distancing within the airport

Airports around the world from Dubai to Amsterdam Schiphol have set up pilot systems to streamline passenger flow. These approaches have relied on centralised biometric databases of pre-registered travellers. They are based on biometric self-boarding systems, which utilise facial recognition technology. Video surveillance at touchpoints inside the airport has also been used.

"This has allowed airport authorities to track passenger movements in a detailed, yet very privacy-invasive, manner. The European Union's General Data Protection Regulation, which requires citizen consent when it comes to processing personal data, has set a new precedent. Observing passengers and scanning a centralised database for facial images is no longer possible," says Koehler, whose company has provided comprehensive biometric solutions on a global scale from Argentina to Mozambique, Fiji to Switzerland.

Currently, biometric documents such as e-passports, commonly used in the EU and elsewhere, require digital reading devices that access information on a contactless chip. This is used to compare and verify the document and its holder. These work at stationary machines set up at checkpoints in the airport, but lead to travellers congregating.

"In the current situation, it would be much better if data reading devices were mobile, creating better traveller flow and distancing within the airport. This is why Mühlbauer has developed systems for the mobile verification of e-passports. These solutions include applications which can be used on a smartphone to easily check electronic travel documents," says Koehler.

"The so-called MB STEEL READER MOBILE app verifies electronic and physical security features such as the visible image, as well as the infrared and ultraviolet images of the document. It can compare the travel document's holder-page information with the data stored on the chip, but also the document data and corresponding records in a database. It is a game-changer."

The app can be used anytime and anywhere inside an airport's security area without disturbing passenger flow. This will be essential as travellers begin to return to airports after the COVID-19 outbreak.

The e-passport continues to be the digitalised anchor of trust, since it holds the traveller's data. Mühlbauer's certified mobile application then accesses the data in the passport's contactless chip and transfers it to the trusted storage of the mobile device. Centralised or decentralised face verification proves the document belongs to the user. Interfaces to external services allow further personal data to be checked. All data is stored temporarily, therefore it's compliant with EU data regulations.

"The application can also be used on standard mobile devices such as smartphones or tablets. High-priced reading equipment or large stationary inspection counters are no longer needed. Airports will be able to utilise space more efficiently and effectively," says Koehler.

"This is just the start. The digital tokenised system can be enriched over time. We could move to a real wallet containing ID and travel documents, tickets, reservations, vouchers, boarding passes and other useful data. It could even be used by officials as a new type of mobile ID. The app also contains all the data elements of an e-passport. There are endless possibilities."

For more information please visit www.muehlbauer.de

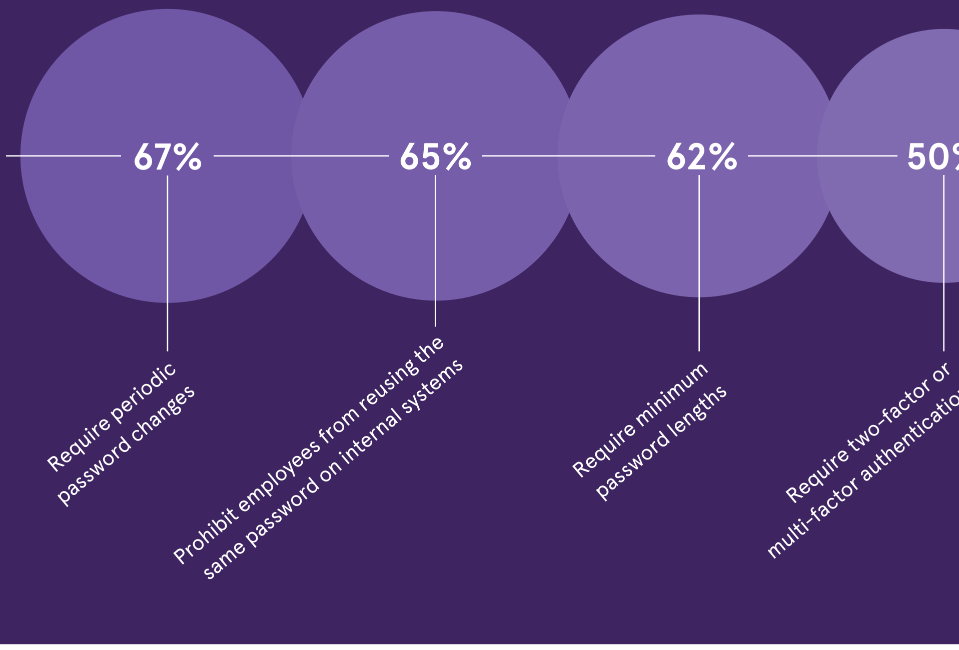
Mühlbauer
High Tech International

AUTHENTICATE AND PROTECT

Unsurprisingly, usernames and passwords are the most common method of authentication when it comes to internal enterprise cybersecurity. But, according to IT professionals, they're not the most secure. This infographic explores the various ways companies are identifying employees and protecting the wider organisation, and how they are taking steps to improve cyber-resilience

STEPS TAKEN TO INCREASE CORPORATE SECURITY

Percentage of organisations taking the following steps



67%

of organisations saw increases in impersonation/business email compromise attacks in 2019

54%

saw increases in phishing

41%

saw increases in internal threats/ data leaks

Mimecast 2019

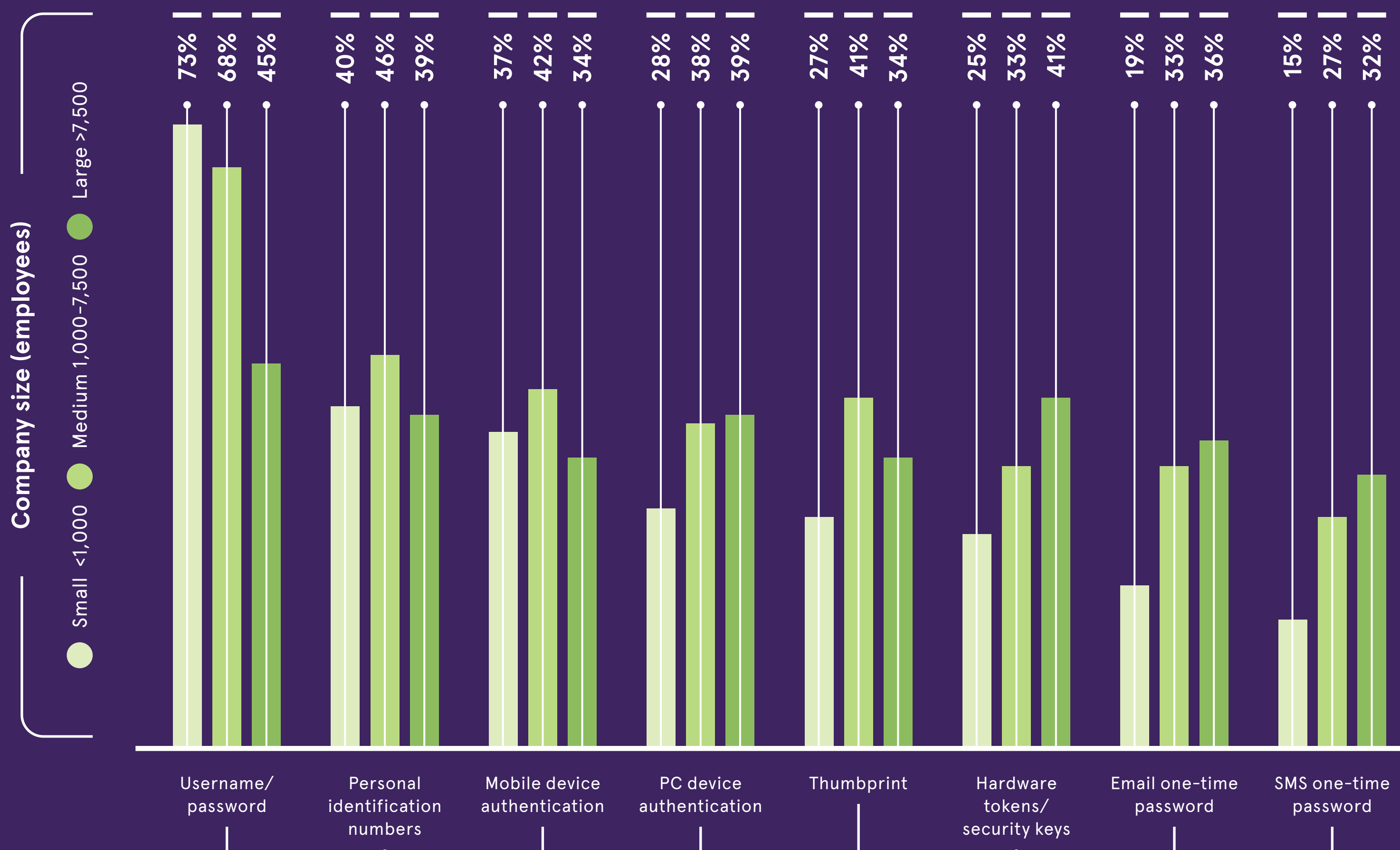
50%

of IT security professionals admit that they reuse passwords across their personal accounts

Ponemon Institute 2020

STATE OF AUTHENTICATION

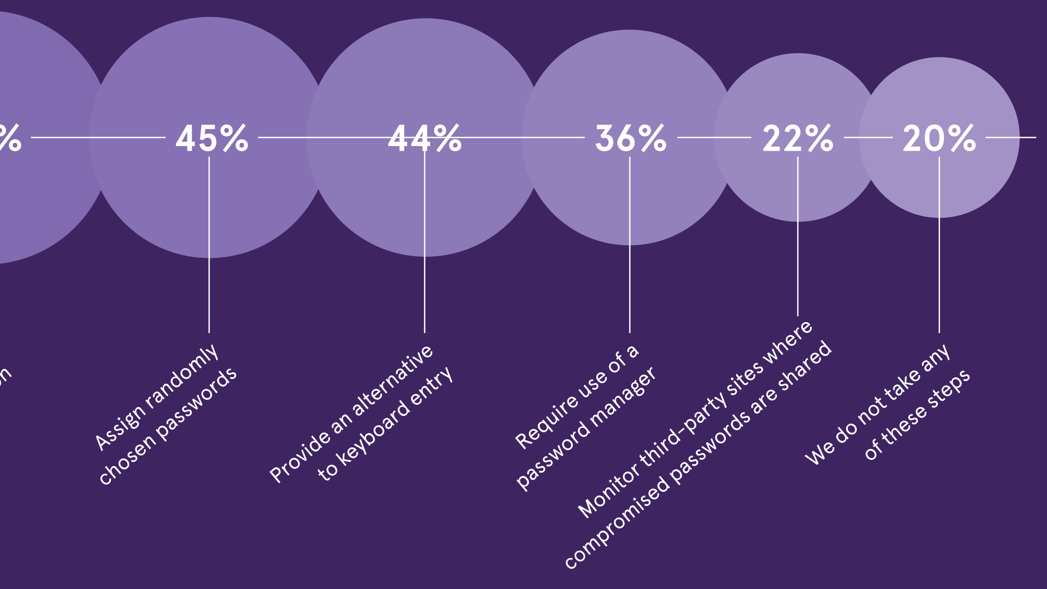
Survey of IT professionals knowledgeable about identity and access management services in their organisation



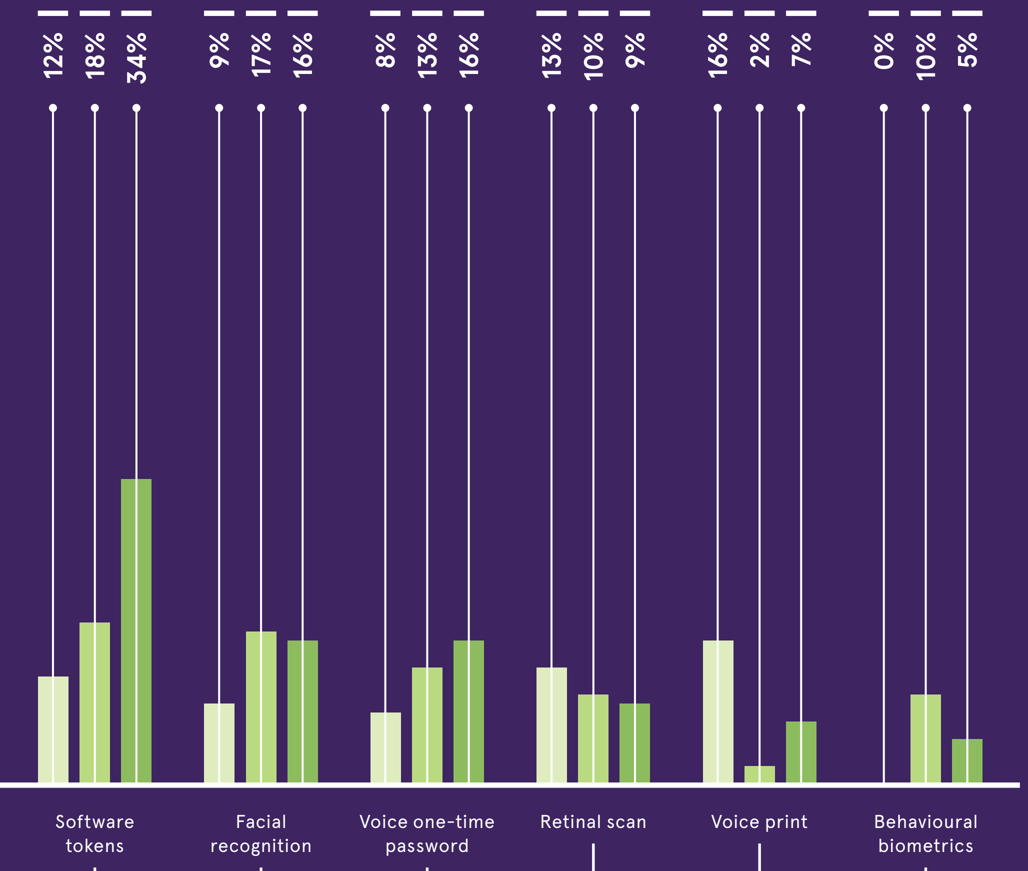
IT professionals' perceptions of security (%)

	Username/ password	Personal identification numbers	Mobile device authentication	PC device authentication	Thumbprint	Hardware tokens/ security keys	Email one-time password	SMS one-time password
Not at all secure	1%	1%	1%	0%	1%	3%	0%	1%
Somewhat secure	13%	9%	5%	2%	4%	3%	11%	7%
Moderately secure	34%	31%	17%	20%	5%	13%	24%	22%
Very secure	29%	28%	41%	41%	22%	35%	42%	41%
Completely secure	17%	23%	29%	29%	43%	37%	18%	22%

Ponemon Institute 2020



Enterprise Management Associates 2019

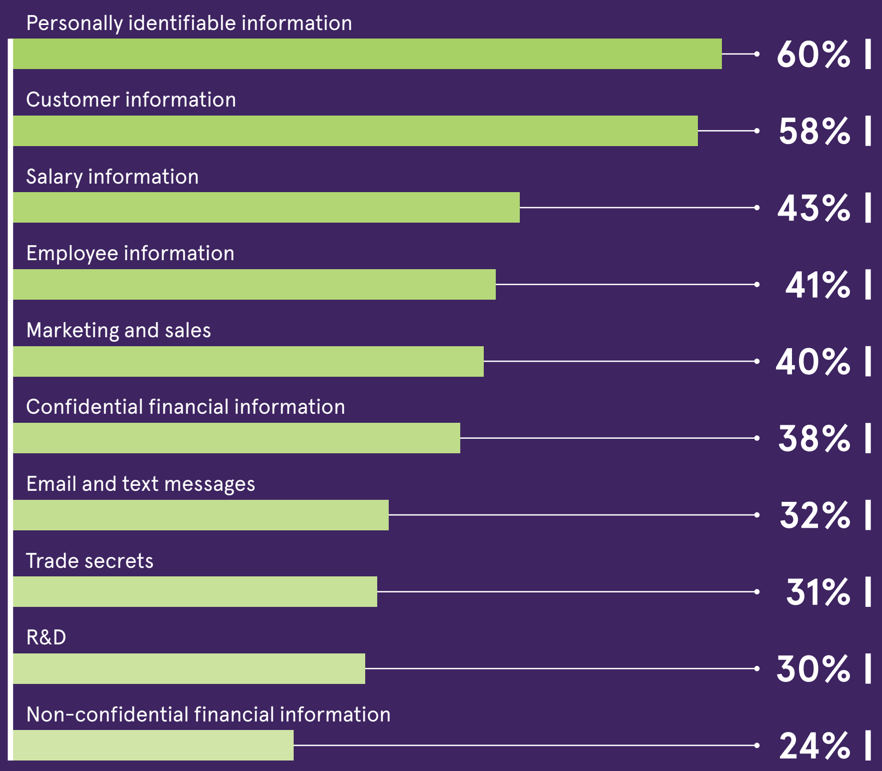


Software tokens	Facial recognition	Voice one-time password	Retinal scan	Voice print	Behavioural biometrics
3%	2%	2%	2%	3%	6%
2%	5%	7%	2%	5%	3%
19%	10%	24%	5%	18%	18%
39%	15%	32%	18%	34%	32%
28%	36%	27%	38%	30%	32%

Percentages do not equal 100 due varying levels of adoption

MOST CONCERNING BUSINESS INFORMATION TO LOSE

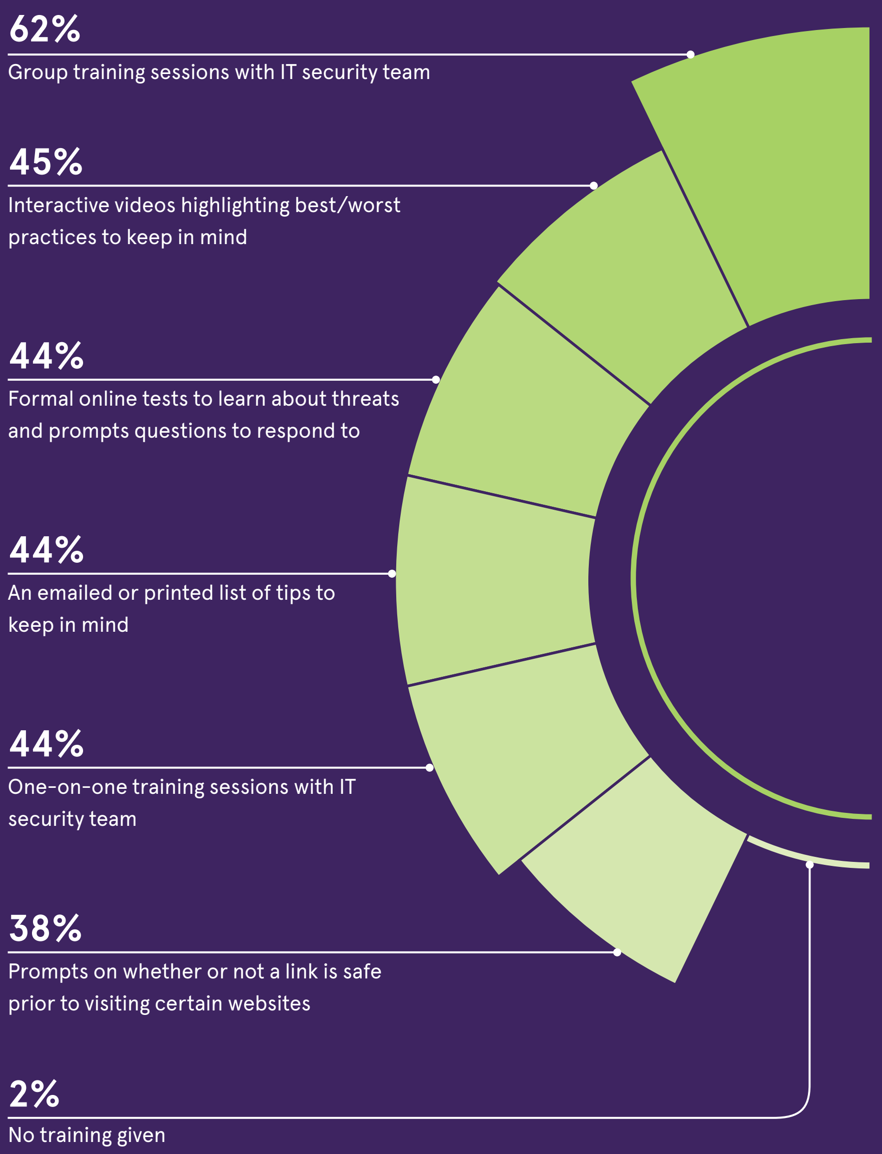
Top types of business information that IT professionals are concerned about protecting



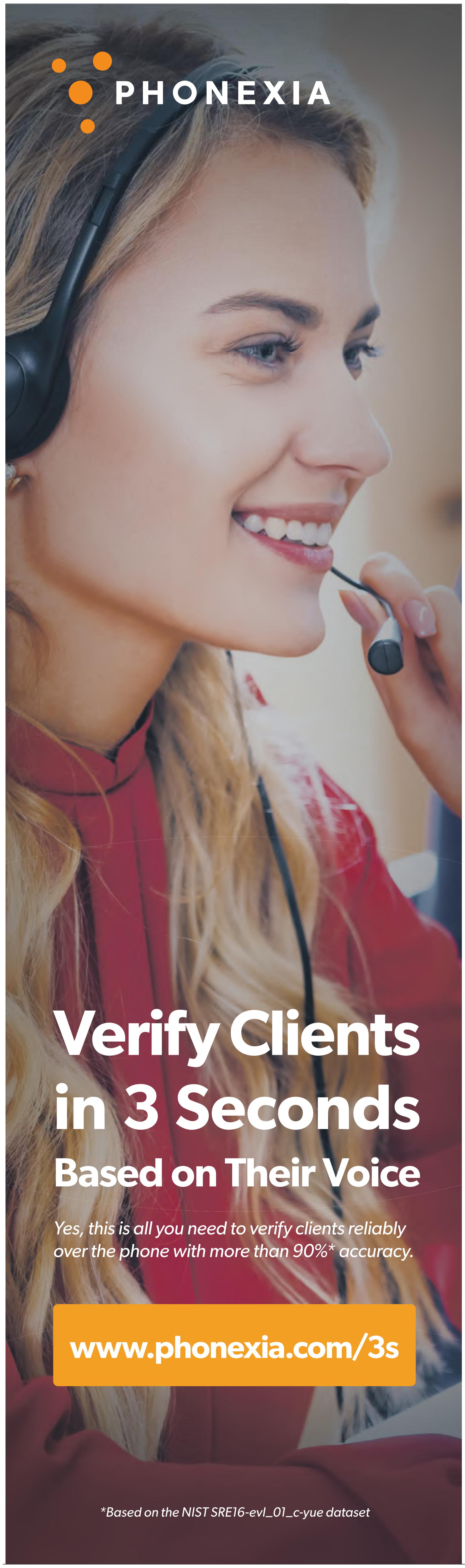
Ponemon Institute 2020

TYPES OF CYBERSECURITY AND AWARENESS TRAINING

Percentage of organisations offering employees the following



Mimecast 2019


PHONEXIA
Verify Clients in 3 Seconds
Based on Their Voice
Yes, this is all you need to verify clients reliably over the phone with more than 90%* accuracy.
www.phonexia.com/3s
*Based on the NIST SRE16-evl_01_c-yue dataset

POLITICS

Biometrics and global ‘regimes of truth’

Depending on where you are in the world, the political landscape is likely to determine whether or not the public embraces civil uses of biometric authentication as a force for good or sees it as an enabler of mass surveillance

Nick Easen

Politics the world over, from the UK to China, Estonia to America, has a huge influence on how biometrics are deployed. Our relationship with the state colours our acceptance of mass surveillance. It determines who we trust with our data and digital identities. In turn, this governs adoption rates for the latest authentication technologies. All these elements are connected.

“We see a push for the development of these technologies from a range of centres of power in the world, from the Chinese state, to the United Nations Security Council, to initiatives from the World Bank. Similarly, the globalised nature of the biometrics industry is itself a driver of deployment,” explains Gus Hosein, executive director of Privacy International.

Each nation is different. Freewheeling, western libertarian democracies spend years debating the checks and balances needed before deploying and regulating biometrics. While a collectivist spirit in some Southeast-Asian democracies encourages civic-minded, yet relatively quick, adoption of the technology, centralised authoritarian regimes can bypass public debate, act rapidly and deploy state-of the-art solutions that drive change.

“This means policy and the adoption of new tech can go from concept, to conceptualisation, to operationalisation at a speed which greatly outpaces that of any other nation following a non-authoritarian regime,” says Dr Patrick Scolyer-Gray, a socio-technical expert from Australia.

This debate is raging right now concerning the coronavirus and use of surveillance technology. Digital apps that share personal data and track your health status are slowing the spread of COVID-19 in Southeast Asia. The United States and Europe are scrambling for similar solutions, with fears being raised on data-rights issues.

“We may find the public become more tolerant of giving up some of their individual privacy rights for the sake of the greater good, such as contact tracing of infected individuals, or for the sake of a different type of individual right, which has suddenly become very precious to us: the right to move around freely in public,” says Tamara Quinn, partner at law firm Osborne Clarke.

Extolling the benefits of biometric and authentication technology to either a compliant or a questioning general public are key, whether you’re in Wuhan or Wolverhampton. If you believe it’s a force for good either after deployment or before adoption – that it will fight COVID-19, for instance – adoption rates can be higher. “For mass surveillance to work, you need people to integrate the technology into their regime of truth,” explains Scolyer-Gray.

If you look at countries where governments have legislated and promoted new technologies both in public and private spheres of life, whether it’s in renewable energy, artificial intelligence, 5G telecoms or fintech, those sectors have flourished. Authentication technology is no different.

"With biometrics, there’s a lot of focus on the data privacy legal issues, but intellectual property law is also key and we could find the two are related,” says Quinn.

“If developers in countries with weak regulatory oversight can innovate biometric authentication

> “
> The polarisation of politics... adds to the perception of a widening gap between security and rights

Ivan Abreu/SOPA Images/LightRocket via Getty Images

A protester destroys a surveillance camera during a pro-democracy march in Hong Kong last September

technology faster than those in countries with stricter rules, such as Europe with its General Data Protection Regulation, they could get patent protection and use it to prevent or control use of that cutting-edge technology around the world."

Some argue that the politics of a given country doesn't necessarily change whether biometrics are developed, but it does affect how it's developed and by whom. This leads to a bigger question of who you trust within society: the government, businesses, both or neither, to spearhead its advancement?

"An authoritarian state might be more closely involved in its development. But a more democratic state is likely to promote private companies to develop technologies, often with less oversight. The increasing polarisation of politics in many countries adds tension to this debate and the perception of a widening gap between security and rights," says Dr Garfield Benjamin, a researcher at Solent University.

This is where strong regulation is playing a part. Adoption rates for authentication technology can be greater where there's more recourse with the authorities if systems go wrong. Protecting people's rights doesn't have to hamper technology development. They can go hand in hand.

"Achieving a balance is possible," says Rocio de la Cruz, principal associate at law firm Gowling WLG. "It requires the organisation implementing this technology to be thorough. They have to be disciplined and committed, as well as constantly involved in the assessment of data protection obligations. They also have to be proactive in the deployment, implementation and review of any necessary measures to do with data privacy and keeping consumers regularly informed."

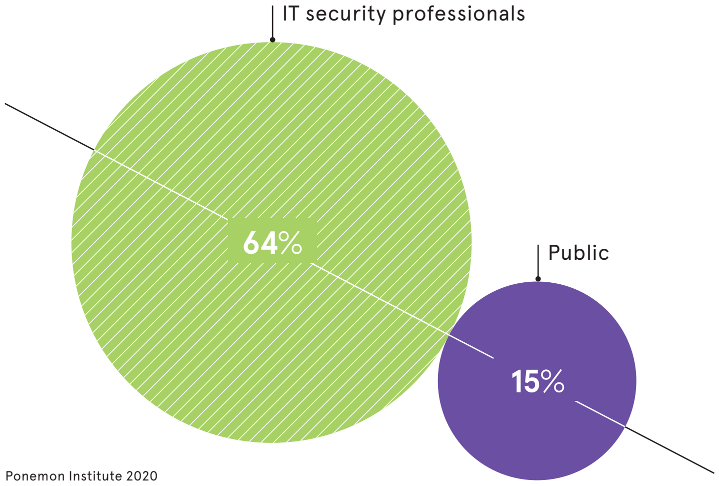
A lot of the issues stem from whether a great deal of thought has been put into deploying systems, or not, and whether people's concerns are addressed. "Biometrics are certainly useful to people. We use them every day. We don't look at this class of technology and presume they're all evil," says Privacy International's Hosein.

"They certainly vary; fingerprints, facial and DNA are particularly challenging because of their links with policing. But mostly the problems come in the implementation. Which biometric system? Where does the data reside? How can the data be reused? How is oversight done? What happens when it fails?"

The recent hacking of Clearview AI, a New York-based facial recognition company, with a database of more than three billion photographs from Facebook, YouTube and Twitter, raises some of these issues. The company listed law enforcement agencies as its clients. It is likely that future data breaches in this sector will raise more questions. "Trust will always be a primarily political and social issue. This won't change," Benjamin concludes. ●

CONCERNS ABOUT GOVERNMENT SURVEILLANCE

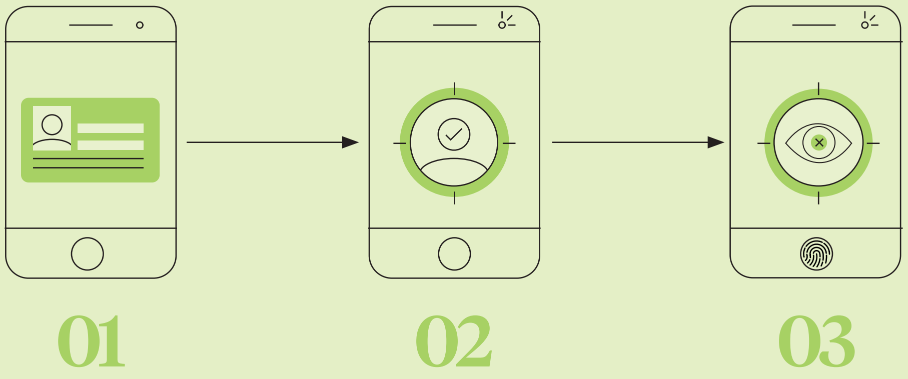
Asked about the top reasons for the increase in concern about privacy and security, the following groups said they had growing worries about government surveillance



Ponemon Institute 2020

Commercial feature

THREE STEPS TO REMOTE CUSTOMER ONBOARDING



Capture identity document:
AI-based ID data extraction with over 99 per cent accuracy

Take a selfie:
Face capture and biometric verification versus ID face portrait

Presentation attack defense:
Liveness detection to defend against presentation attacks

Secure technology for building instant trust from Innovatrics

Remote customer onboarding is no longer just a nice to have

Instant biometric authentication, through successful digital onboarding, is now more crucial than ever

If the coronavirus outbreak has shown us anything it is that we're moving to a more connected, online world in which we need to prove our identity securely. Biometrics will be in high demand. Take onboarding practices with traditional banks, this involved visiting a local branch to verify who you are with ID documents. Not anymore, so remote access to services via a customer's device will be critical.

"With most countries across the globe implementing stay-at-home policies, we see banks and telecommunication firms, even governments, moving beyond traditional verification and investing in remote digital onboarding using biometrics, other technology powered by artificial intelligence," explains Donal Greene, head of enterprise at Innovatrics, a global leader in biometrics, which has enrolled more than a billion people worldwide.

"Those that don't will lose out to digital-first challenger banks during these testing times. That's why many global financial institutions and established players are falling behind.

"Right now, financial service providers across the globe are clamouring for safe and secure digital authentication of new and existing customers. The volume of inquiries has increased significantly as they rush to offer more digitalised services online and via mobile apps, especially in response to measures like social distancing."

Digital-first and challenger finance providers in developing regions from Southeast Asia to Africa have been early adopters, banking the unbanked and bringing microfinance and responsible lending to millions. Their experience demonstrates that onboarding, the process of capturing and verifying a new customer on a digital platform, must be effortless and seamlessly integrated into a bank's existing infrastructure to maximise efficiency.

"There may be a perception that UK and European banks are ahead with digital initiatives. It's just not true. We are using our Digital Onboarding Toolkit to enrol millions in developing economies. We've been enrolling 30,000 a day in some markets. It takes less than five minutes. You need a service that is quick, easy to use and able to detect fraud rapidly," says Greene.

"We use proprietary state-of-the-art algorithms trained on millions of datapoints. Our algorithm for face identification is the fastest in the world and among the most accurate. It only takes 13 milliseconds for the algorithm to identify the correct face in a database of 12 million enrolees."

Biometric identity verification will be one of the most important investments for many companies in the coming decade. Yet the market for digital onboarding is becoming increasingly crowded. There are many providers. It is difficult for banks and other finance providers to assess the right biometric technology partner.

Greene says: "The key is to look in depth at the biometric technology being used. Is it proprietary? Can it be customised and scaled? Has it been benchmarked and certified? Will it be compliant with local data, financial and anti-money laundering regulations? More importantly, is the technology user friendly and intuitive?

"Sixty per cent of our resources are focused on research and development to advance our technology using machine-learning. The key aim is to improve the user experience, increase accuracy and get smarter at reducing fraud. The most important element here is to adapt technology to humans and to efficiently address digital age business needs.

"Innovatrics has been active in this market for 16 years with more than 500 projects in 80 countries. It holds a unique place in the remote onboarding ecosystem. All our technology is proprietary and top ranked in the relevant benchmarks. This means companies don't need to deal with several vendors and integrate multiple technologies to build a remote onboarding solution."

So, what does the future hold? Greene says it is an evolution, not a revolution. Biometric technology is getting faster, more accurate, more secure and relevant to a wider range of use-cases. The future is exciting.

For more information please visit www.innovatrics.com

INNOVATRICS

FACIAL RECOGNITION

Why racial bias in facial recognition still exists

Using limited datasets to build facial recognition technologies, with images that don't represent society as a whole, has prompted an ethical debate about their evolution

Peter Yeung

With technology capable of matching billions of fingerprints a second, scanning retinas with infrared light to record the unique DNA pattern of blood vessels and live cross-checking faces with millions-strong databases, biometrics ethics has become an increasingly important area.

Governments, police forces and enterprises across the world have for various reasons come to adopt biometrics technology to identify individuals based on biological and behavioural characteristics, particularly in the context of the COVID-19 epidemic when in-person verification may not be possible.

Yet this pioneering field has been mired in concerns surrounding privacy, human rights and systematic prejudice, with some biometrics technologies, such as facial and voice recognition, shown to produce racial and ethical bias that could see innocent people jailed or refused essential welfare benefits.

Carly Kind, director of the Ada Lovelace Institute, an independent research body that monitors artificial intelligence (AI) and data ethics, says this is largely down to flawed or limited datasets used by companies.

"It comes down to bias in the data that informs the system," says Kind. "This originates from unrepresentative datasets and this may be because the developer of the technology hasn't ensured there is a proper representation of ethnicities, genders or social classes."

The empirical evidence is stark. A groundbreaking study published in December by the US-based National Institute of Standards and Technology, which analysed 189 software algorithms from 99 developers – the majority of the industry – saw higher rates of inaccuracy for Asian and African-American faces relative to images of Caucasians, often by a factor of ten to one hundred times.

It followed research in 2018 by the MIT Media Lab, a research laboratory at the Massachusetts Institute of Technology, that found leading facial recognition systems by Microsoft, IBM and Megvii of China performed at a 0.8 per cent error rate when used on images of white men, but at a rate of 34.7 per cent when tested on images of dark-skinned women.

MIT researchers pointed to the imagery datasets used to develop these facial recognition technologies, found to be 77 per cent male and 83 per cent white, as the reason behind the disparity in performance.

02

Matthew Horwood/Getty Images

01
Racial bias in facial recognition technologies have prompted concerns about the use of the software by police

02
A police facial recognition camera in use at the Cardiff City Stadium

"It's very difficult to reach a point where you have a completely objective dataset that is perfectly representative and unbiased," says Kind. "But it can be dramatically reduced."

However, Pawel Drozdowski, a researcher at Germany's National Research Centre for Applied Cybersecurity, the largest of its kind in Europe, believes there are potentially more complex reasons behind biometrics ethics.

"There is a perception that with more training data we could eradicate bias and to some extent that's true, but not completely," he says. "Because isolating the actual source of bias is very challenging."

According to Drozdowski, behavioural cues and variables such as lighting, distance from the facial recognition sensor and whether a person is wearing make-up can seriously impact the efficacy of biometrics.

"These systems are often built for men, who are on average taller than women," he explains. "Therefore, the position of cameras aren't optimised for them, leading to a worse performance of the technology."

The dearth of balanced data available for companies is also a stumbling block for improving biometrics ethics. Data protection laws, such as the European Union's General Data Protection Regulation, supported by a wave of public opinion, have limited access to and handling of personal information. "We just don't have enough data," adds Drozdowski.

One approach to improving biometrics ethics by UK-based biometrics company Onfido has been to only use data provided by and with the consent of clients in creating its algorithms that protect against identity fraud.

> **“**
> **Most training datasets only use photos of celebrities because they're easier to find. But these aren't representative of the world**

Nicholas Green/Unsplash

34.7%

error rate of leading facial recognition systems when analysing images of dark-skinned women, compared with an error rate of 0.8 per cent when tested on white men

Analysis of 1,270 faces to determine the accuracy of gender identification dependent on skin colour

MIT Media Lab 2018

10-100×

more likely for facial recognition software to inaccurately identify Asian or African descent faces compared with Caucasian people

Analysis of 189 software algorithms from 99 developers

National Institute of Standards and Technology 2019

"We don't purchase any data, we don't scrape the internet for any data, we don't pay people to generate data," says Susana Lopes, the company's director of product. "Because we are tied to whatever our clients agree to share with us, this means our database is representative of our client base."

Onfido's concept is to use AI-based technology to assess whether a user's official, government-issued ID is genuine or fraudulent and then compare it against facial biometrics of the user, in theory verifying their identity and physical presence.

Lopes says demand for Onfido's services has surged in recent weeks with online healthcare work quadrupling. But even with such growth, she concedes: "It's going to take longer to acquire datasets that are as balanced as they need to be."

Other companies have taken more innovative and costly routes to reduce and prevent systemic bias in biometric systems.

Brent Boekestein, chief executive of Vintra, a California-based video analysis company, says its custom training database was created "from the ground up" in an effort to mitigate any potential bias.

"Most training datasets only use photos of celebrities because they're easier to find," says Boekestein, in reference to MS Celeb, a dataset of ten million face images harvested from the internet. "But these aren't representative of the world and tend to be beautiful; they tend to have high cheekbones and they tend to be younger."

Instead, Vintra's dataset has been constructed with a diverse selection of public figures from around the world, such as African first ladies, thereby avoiding security or privacy concerns. It contains more than 20,000 identities taken from 76 countries, equally balanced across ethnic groups. "It took us a long time and cost us a lot of money, but we built a more holistic view of society," says Boekestein.

Since 2018, the company has reduced the gap between the most (Caucasian) and least (African) accurate performance on ethnic groups from 11.9 per cent to 3.5 per cent, with an average accuracy now of 89.2 per cent, surpassing the leading commercially available competition by Microsoft and Amazon.

Despite these improvements, human rights campaigners oppose the technology due to the problematic state of biometrics ethics. "While inaccurate biometric surveillance presents clear dangers, a more accurate version of facial recognition also presents severe risks to our fundamental rights," says Hannah Couchman, policy and campaigns officer at Liberty.

But it appears it will only be a matter of time before biometrics become an ever-greater part of our lives, from policing to electronic banking and citizen services. Almost all of India's 1.25 billion population is already part of the national ID system, the largest biometrics system in the world.

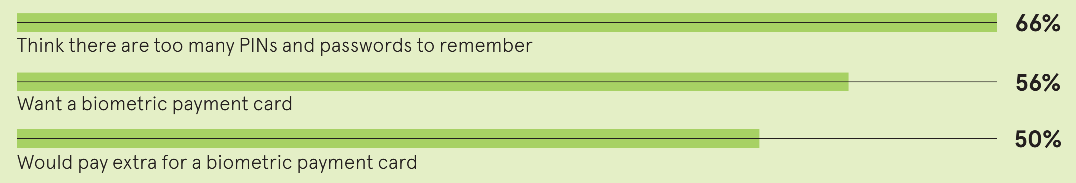
Researcher Drozdowski believes the technology's potential for good, such as finding missing children or identifying active criminals, must be balanced with safeguards. "Oversight is a big part of biometrics and any sort of automated decision-making," he says.

Kind at the Ada Lovelace Institute agrees, suggesting the need for continuous risk assessment and awareness of these systems' limits.

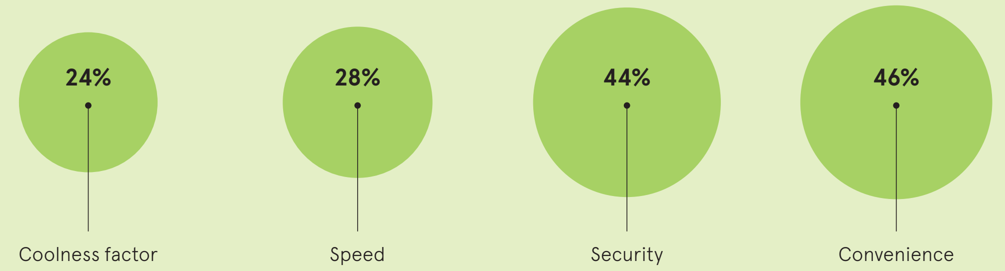
"Biometric technology can absolutely be used for positive ends," she adds. "But it is going to create real societal and ethical questions, and you have to engage with workers and employers to understand what is being traded off and what is being gained." ●

Commercial feature

CONSUMER SURVEY RESULTS



MAIN BENEFITS OF BIOMETRICS, ACCORDING TO CONSUMERS



Survey conducted with 1,200 consumers in the UK, France and China by Kantar TNS for Fingerprints

Market for biometric cards is unstoppable

Biometric payment cards look set to surge as the coronavirus impacts shoppers

Growth in contactless payments began before the coronavirus outbreak, but increasing spending limits have raised questions about security. However, the pandemic is likely to drive greater use of biometric authentication, which is already being seen with mobile payments across the globe.

The World Health Organization has urged people to use contactless payments instead of cash at a time when the UK has raised its contactless limit to £45, alongside similar increases in other countries. But with no increased security. This has the potential for more fraud, yet the limit is still too low for a family's grocery shopping. The need to enter a PIN, which is easily forgotten, is also a second-rate user experience. Research shows consumers are tired of PINs and passwords.

"Globally, there's a real need right now for biometric authentication, for both payments and access, whether it involves fingerprints or iris scans," says Christian Fredrikson, chief executive of Fingerprints, a Swedish company that`s shipped more than a billion fingerprint sensors. "At the same time, hacker intelligence and tools are getting better. We must stay one step ahead. Presently, PINs and passwords are ridiculously easy to hack."

To date 21 banks around the world are piloting contactless biometric payment cards on both Mastercard and Visa networks, including Natwest and RBS in the UK, and there's also been a commercial launch in Switzerland, all using Fingerprints technology. The main benefits are higher levels of security and convenience, since you don't need to enter a PIN, and greater speed.

"Consumer feedback has been really positive. The majority would like to have this card in the future and would recommend it to a friend. There's even a willingness to pay for a biometric card. There's now a strong drive from the global banking ecosystem to launch this," says Fredrikson, whose company is the largest supplier of biometrics to the global banking industry.

"There are also security, data and big brother concerns, but in the case of biometric contactless payments, you're not sharing your personal data with anyone, it doesn't leave the card. The consumer's data is encrypted, matched and verified on the card when payments are made. Biometric authentication is a really safe way to deal with the payment cap."

Biometrics have already achieved huge success in the mobile market. Nearly three quarters of all smartphones sold have biometric authentication built in and more than 80 per cent now use it to unlock phones, secure apps and make payments. Fingerprints also works with eight of ten top global mobile device manufacturers to facilitate their authentication technology.

"We've seen tremendous growth in biometrics in smartphones; it's only a matter of time before this comes at scale to contactless card payments. We also see huge benefits in other sectors too, where passwords are not the answer and can be easily hacked, such as remote and home working with secure login to company systems, and entry into buildings with touchless biometrics or biometric access cards. This trend is set to continue," says the chief executive of Fingerprints, which authenticates more than ten billion touches on its sensors daily.

Earlier this year the NHS looked at upgrading its authentication technology for computer logins by employees, replacing passwords with biometrics such as fingerprint access.

"Touchless access will be even more vital in this coronavirus-aware era. The big issue is the 'dilemma of opposites': the public want 21st-century, top-grade security, but they also want total convenience. Biometrics is the only answer to marry the two," says Fredrikson.

Awareness of the benefits of biometrics is growing. How fast will it be adopted? Only time will tell. History has clues. It only took eight years to reach a billion contactless cards. This needed new payment infrastructure. For biometric cards this isn't necessary as they already work in contactless terminals. Therefore, the rollout will be faster. "Biometrics brings huge benefits to many industries. The market is truly unstoppable," Fredrikson concludes.

> "Touchless access will be even more vital in this coronavirus-aware era

For more information please visit fingerprints.com

FINGERPRINTS

BIOMETRICS

Busting six common myths about biometrics

Biometric technology could transform digital authentication, but misconceptions about privacy breaches, accuracy levels and security risks may hinder its widespread adoption

Alexandra Leonards

Trismegist San/Shutterstock

"Biometric data is stored as whole images, so hackers can access my face and fingerprints"

Biometric data is initially extracted from an image, but the image itself is not what's used in the authentication process. The original sample, whether it's an image of a face, fingerprint, iris or otherwise, is quickly discarded and replaced by a mathematical file called a biometric template. The template is a digital reference of the unique characteristics found in that initial image.

"The characteristics of a biometric such as a face or fingerprint can be encoded mathematically into a much smaller representation that is easier to store and test against," explains Kevin Goldsmith, chief technology officer at Onfido. "This mathematical representation is still considered personal data because it is unique to a person, but it doesn't let a hacker see a photo of a face or fingerprint."

There are a number of methods used to safeguard these biometric templates, including distributed data storage. This technique stores smaller, encrypted biometric data in a number of locations, like on a server and a smartphone.

"Having biometric data encrypted in this way renders it useless to a hacker," says James Stickland, chief executive of Veridium. "This can be done without making any organisation the custodian of the data, as biometric templates can be stored in a decentralised location, leveraging this distributed model and effectively minimising the risk of a data breach."

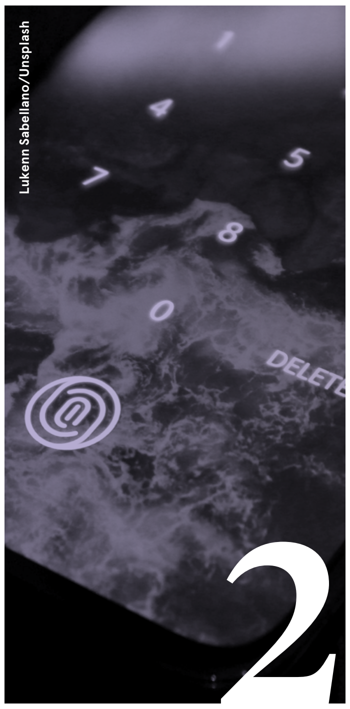
"Biometrics are easy to replicate"

It is possible to duplicate biometric data in the form of a fingerprint or face by using methods such as 3D-printed fingerprints or replica heads, but it's certainly not easy or commonplace.

In general, biometric technology incorporates a number of features or stages in the authentication process. A fingerprint, for example, is often combined with a contextual signal like fake device detection or expected location.

"Despite what we see in *Mission Impossible* or similar action movies, biometrics are actually quite difficult to replicate," says Dr Toby Norman, co-founder and chief executive of Simprints. "The large majority of vendors have implemented liveness detection and other forms of anti-spoofing within their solutions that render it increasingly challenging to fake a biometric."

Liveness detection algorithms can analyse images to distinguish between a bogus attempt made by someone using a reproduction and an authentic attempt made by a live human being.



Lukenn Sabellano/Unsplash

Vitalii Vodolazskyi/Shutterstock

"Biometric data is unreliable and error rates are high"

Sceptics may question the reliability of biometric technology, but evidence shows it's far superior to outdated methods such as password authentication.

Password verification accounts for more than 80 per cent of cyber breaches, according to a recent Verizon report. Biometric technology on the other hand boasts much better security performance and high accuracy levels.

Decades of technological advancement mean fingerprinting has accuracy of more than 99 per cent, according to a study by the National Institute of Standards and Technology (NIST). Iris scanning is even more precise. A report by the Government Office for Science found low error figures imply that for every 100,000 iris scans, only two mistakes are made.

"By moving away from measures based on what you know, which can be phished and stolen, and instead pairing these with innovative biometrics, such as the way a user interacts with their device, organisations can strengthen security in a way that is frictionless, reliable and transparent," says Stickland at Veridium.

However, it is worth noting that although biometrics is largely reliable, it isn't perfect. Artificial intelligence-based technology such as facial recognition is still hampered by racial biases. A recent NIST study of facial recognition algorithms in the United States found that Asian and African-American people were up to 100 times more likely to be misidentified than white men.

SFIO CRACHO/Shutterstock

"Companies can share my data without my knowledge"

Under data protection law, you have the legal right to be informed about how your personal data is being used. You can also legally halt or restrict the processing of your data and object to how it is being processed in certain circumstances.

According to the European Union's General Data Protection Regulation (GDPR), sharing personal data can only be lawful if either consent is given or another legitimate basis exists. Examples of situations in which permission would be bypassed include when the data is needed to save a person's life, when the information is required to comply with a legal obligation or when sharing that information is in the public interest.

"Except for a few very special cases, informed explicit user consent for any use of data is obligatory," explains Andrew Bud, chief executive of iProov.

Biometric data has even stronger legal protection. It is one of nine special categories outlined in the Data Protection Act 2018, the UK's implementation of GDPR, which means companies processing biometric data must have both a lawful basis and meet an additional condition to do so.

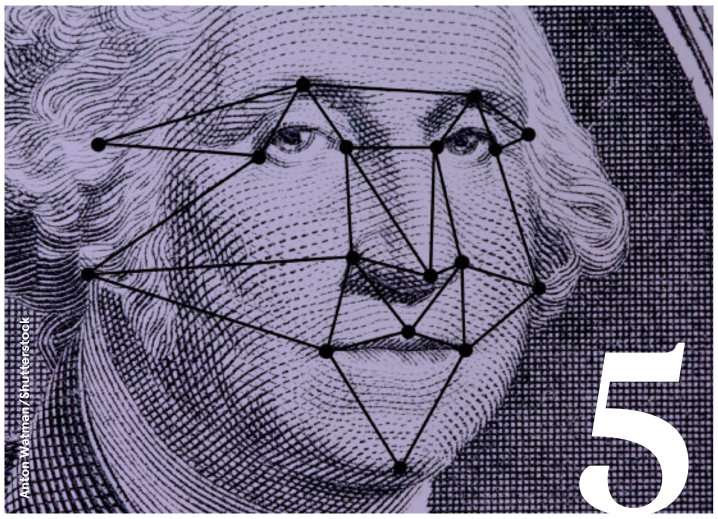
“Biometrics are expensive and aren’t cost effective in the long run”

Advances in technology mean the cost of biometrics is falling all the time. “Ultra-accurate face verification is now more or less free in the cloud from vendors such as Microsoft, Amazon and others,” says Bud at iProov. “This makes it possible for even small companies to develop very high-performance systems that cost very little to run.”

The benefit of bring-your-own-device strategies, which leverage widely adopted smartphones, mean biometric platforms require very little initial investment. “Plus, over time, the cost benefits will snowball; there are no additional fees to onboard new employees and no expensive hardware to regularly upgrade,” says Veridium’s Stickland.

As a result of what’s commonly known as “password fatigue”, many users are regularly resetting passwords and calling IT helpdesks. Veridium estimates that businesses with 10,000 employees spend around $1.9 million annually on password resets. So swapping or enhancing traditional password authentication with biometric data can also mean big cost-savings for businesses.

According to a report by the UK’s Department for International Development, when Nigeria launched its e-ID system it made an annual saving of $1 billion through exposing 62,000 so-called ghost workers in the public sector.



Anton Watman/Shutterstock

“Biometrics take longer to process than other forms of authentication”

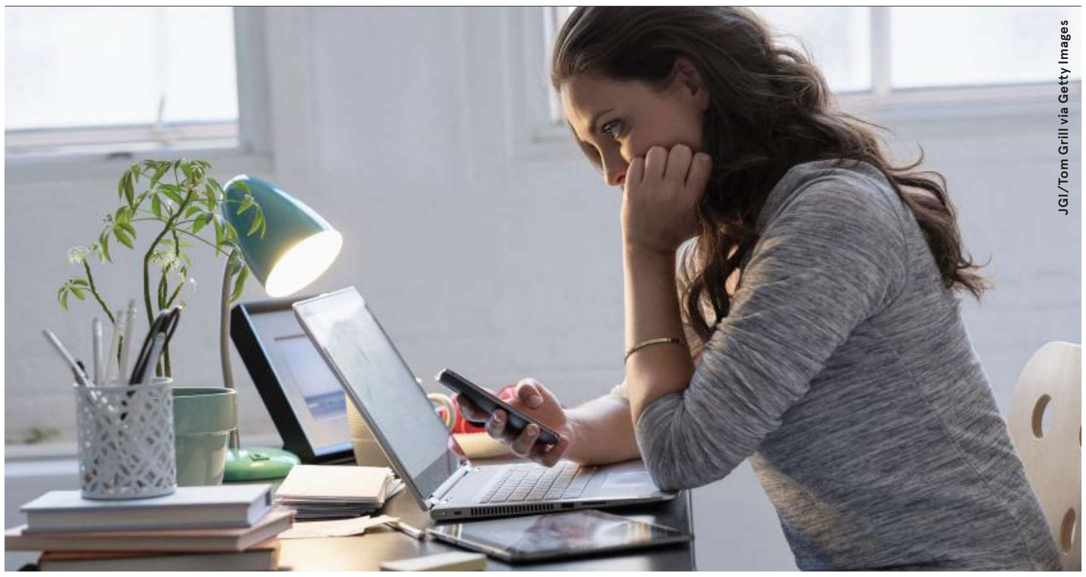
Processing biometric data can be every bit as quick as other methods of verification and is faster in many cases.

“Typing in a password or getting a two-factor authentication code from an application, SMS or hardware key is substantially more time consuming than using a fingerprint or taking a selfie to authenticate,” says Goldsmith at Onfido.

As Anton Klippmark, product marketing manager at BehavioSec, points out: “The big premium is on gaining biometrics’ and behavioural analytics’ powerful anti-fraud data, without adding friction to the user experience, because if new security measures are too cumbersome to use, it breaks the mobile and convenience-based business models of apps and services.” ●

1000 Words/Shutterstock

Commercial feature



JGI/Tom Grill via Getty Images

Removing friction from authentication

Organisations have sought to ramp up their authentication measures to combat more sophisticated threats, but adding friction causes unnecessary damage to user experience

Credential stuffing, whereby automated systems are used to access user accounts with stolen usernames and passwords, has exploded as cybercriminals have adopted increasingly intelligent and sophisticated methods to circumvent the traditional countermeasures deployed by organisations.

In particular, hackers are deepening their capabilities around imitating legitimate users. They use the same tools that users do, automating production browsers, such as Chrome, Firefox and Safari, and proxying through residential IP addresses.

By emulating human traffic and behaviour, they can bypass lower friction defences, multi-factor authentication, or MFA, gates and rate limits to takeover accounts, crack cards or steal data. Malware sits resident on victims’ computers, scraping their credentials and delivering them back to fraud marketplaces.

Intelligent phishing proxies, which seamlessly skin over a legitimate website and then intercept the traffic that goes through, are also on the rise. Users are fooled into thinking they are logging into their email account or online banking, as the web page looks the same, but meanwhile their credentials are being stolen by a cybercriminal. In response, organisations have been drastically stepping up their authentication layers.

“Five years ago, it was not uncommon to find that the only way an organisation was authenticating users was through a single login form on a webpage. Fraudsters had free rein passed that point,” says Jarrod Overson, director of engineering at Shape Security. “Now, MFA is commonplace, we’re seeing more magic links and then even past the first login gate, companies are increasingly risk-scoring each user’s behaviour to assess whether they need to be authenticated further.”

Security ≠ friction

While organisations have undoubtedly added more security to their authentication, they’ve also added more friction to the user experience. CAPTCHA tests (completely automated public Turing tests to tell computers and humans apart) are frequently derided on social media networks as a painful process for proving human identity, while even MFA causes a significant level of disruption to a customer journey, even more so if the user doesn’t have their smartphone to hand.

This additional friction comes at a time when IT, marketing and sales departments are already eroding the seamlessness of their digital channels, whether through pop-ups urging people to accept privacy policies, user session tracking or customer journey mapping. When companies then start to apply security on to those applications, it can easily feel like they are imposing a dramatic amount more friction than is necessary.

Organisations that add a lot of friction to mitigate fraud may incorrectly think they are improving security defences. Meanwhile, however, they are likely to be overlooking the downstream damage they’re causing to their customer experience. Too much friction can negatively impact account creation, logins and conversion rates. More worryingly, they’ll soon find their social media pages are being blighted by poor reviews that damage their brand and reputation, and ultimately soon their sales will be affected.

“Companies need to architect a better balance between security and user experience,” says Overson. “Attackers have started with basic tools that did a simple job and have evolved over the last five years to more convincingly look generically human. Now they are moving towards more aggressively looking specifically human. As defences improved to block questionable behaviour, attackers responded by creating tools to exploit and imitate individual users with all their nuances.”

Shape Security, which protects more than one billion transactions per day from imitation attacks, leverages artificial intelligence and machine-learning to build security and anti-fraud solutions that are completely configurable to the customer application and attacker. This allows companies to reduce friction for their legitimate users while dynamically ramping it up for potentially bad traffic and even more aggressively for actual attackers.

“We’re showing through our solutions that authentication need not come at the expense of customer experience,” Overson concludes. “A combination of layered defences against attackers alongside positive rewards for legitimate users makes it easier to see how additional security can actually improve the overall experience.”

> “
> We’re showing through our solutions that authentication need not come at the expense of customer experience

For more information please visit shapesecurity.com

Part of F5

Alvarez/Getty Images

VOICE

Deepfakes highlight key flaws in voice ID tech

Voice authentication might sound like a more seamless method of identifying an individual, but it isn't yet a silver bullet for financial fraud

Edd Jefferson

Though issues around authentication are key for an ever-growing list of industries, banks and financial institutions perhaps face the most severe consequences of getting it wrong.

Increasingly, they're looking to voice biometrics as a secure and convenient way of providing access to their services. Customers simply have to speak to an authentication system that can recognise unique markers and almost instantly confirm who they are. But is this really the end of bank fraud or simply another challenge for would-be fraudsters to rise to?

Banks face a tricky balance when authenticating customers as the process needs to provide enough security to prevent fraudulent access, while not being so cumbersome that customers have difficulty with, or actively avoid, using the services.

"Which card reader do I need to use for this account?" "Which aunt's birthday is my memorable date for this bank?" Biometric authentication bypasses a lot of these issues by allowing users to present themselves, or at least measurable aspects of themselves, as proof of identity, most commonly their fingerprints, face and voice.

And voice recognition has the advantage of simplicity as the user doesn't need any technology more sophisticated than a landline phone.

Banks and the companies that provide their voice biometrics make bold claims for the ability to distinguish individuals' voices. Hundreds of speech characteristics are analysed, from accent and speed to physical characteristics of vocal chords.

But in practice the technology hasn't always been perfect. In 2017 a BBC reporter and his non-identical twin brother managed to bypass HSBC's system, albeit only after eight attempts. HSBC subsequently claimed to have increased the sensitivity of their system.

However, it's not just a sibling with a similar voice you need to worry about. What if someone tries to access your financial services with your voice or a synthesised version of it?

"Deepfake voice algorithms have already been reported that can perfectly imitate someone's voice using just a five-second snippet," says Ray Walsh of privacy education and review site ProPrivacy.

And the idea that this could be used for financial fraud isn't theoretical. Walsh points to a 2019 incident in which an energy company was tricked into handing over nearly a quarter of a million pounds after phone conversations with what turned out to be deepfaked recordings of their parent company's chief executive.

The deepfake in that incident fooled human beings, not a voice biometrics system. Voice recognition algorithms can't be tricked in the same way that a human on the end of the phone could be. But this doesn't mean they can't be fooled by sufficiently advanced deepfakes, perhaps resulting in an artificial intelligence (AI) arms race, with criminals improving their AI deepfakes and financial institutions tweaking the neural networks that power their own voiceprint detection to keep up.

Deepfakes aren't the only thing that might threaten voice recognition systems as, like the rest of us, they can fall victim to age. Voices change over time; a 2017 study by voice authentication company Pindrop found that over two years the failure rate of authentication more than doubled.

If someone's using a voice biometric service frequently, it's in theory possible to recalibrate the model of their voice you've stored with new information as they sign in, allowing for some compensation for this. But this introduces risks, potentially allowing the mechanism to be more easily compromised.

And banking customers don't necessarily call that often. A survey by Pindrop found almost half of customers only called once in an eight-month period, long enough that vocal changes could prevent the system from verifying the customer, requiring alternative verification methods, which could be more easily compromised.

This can, in theory, be compensated for as neural networks can be trained to allow for the typical effects of ageing. Banking voicetech provider Nuance say their system should theoretically allow for someone to create a voiceprint aged 20 and not have to update it for 60 years, but it will obviously take a while to find out if that's true in practice.

The convenience of voice biometrics as an authentication method makes its appeal obvious, but it remains to be seen exactly how viable the technology will be in the long term. And for now, even if financial institutions are confident in their systems' ability to sniff out deepfakes and predict how voices will change with age, their customers might not share that optimism.

> Deepfake voice algorithms have already been reported that can perfectly imitate someone's voice using just a five-second snippet

After all, a 2019 survey by Paysafe Group found that 56 per cent of consumers in North America and Europe have concerns about biometrics and 81 per cent prefer the traditional password-based approach.

As much as banks are pushing them to, customers may not be quite ready to say that, figuratively or literally, "my voice is my password". ●

OPINION

‘I hope for a future where authentication is seamless… and where passwords are obsolete’

We must stop blaming the user for the failures of authentication technology. As people have been required to manage almost every aspect of their lives through multiple accounts accessed through technology, authentication practices have evolved, but not necessarily improved.

Authentication technologies are not kind to users. Too many layers have been added and it’s not sustainable because people misuse complicated technology. Yet it’s the users, not the technology makers, who get the blame when things go wrong and mistakes lead to a data breach or a compromise of security. Authentication technology needs to be convenient; it must not require technical expertise to use, nor should it lead users to try and circumvent it.

The information security industry is often guilty of trying to force its culture on to everyone else, whether or not those rules make sense in other walks of life. Authentication is a prime example of this.

Let’s consider passwords. Users have long been told to create unique and complex passwords for each individual account they access. We know that the average person in the workforce has almost 200 accounts requiring passwords, making that advice absurd. To make things even harder, we’ve told users that they are not allowed to write their passwords down. In theory, I understand the intent behind this, but in reality, what’s more likely: someone breaking into your house and stealing the piece of paper with your passwords on, or someone brute-forcing or guessing your password online?

I hate the security-versus-convenience debate and its suggestion that we have to choose between the two, and when it comes to authentication specifically, it riles me even more. Consumers deserve an easier experience and should be able to utilise their power as consumers of products, services and sites to demand a less stressful and more convenient authentication experience.

It’s easy to lament all of the mistakes made by the industry and the various shortcomings when it comes to authentication, but it’s a lot harder to accurately predict its future.

Shared authentication certainly ticks a lot of boxes in the convenience column, but lacks in security. If your Facebook or Google account is compromised, for instance, all other accounts authenticated using those platforms would be vulnerable too. We all know about eggs and baskets.

Touch ID and Face ID on phones is another indicator of the direction in which authentication is going, but biometric use carries concerns around privacy, politics and of course in the instance that the biometric authentication fails, it refers you back to enter your passcode. With authentication only as secure as the weakest authentication option, this is therefore ‘biometric for convenience’ as opposed to an increased level of security.

Design needs to play a big part in the future. Authentication design needs to be simpler, more usable and create far less friction and frustration for the user. Attractive design could even encourage security adoption, with the authentication process becoming desirable rather than dreaded.

On a more technical level, the future of authentication will likely rely on algorithms to determine a user’s identity and ultimately detect fraudulent behaviours and actions. It should be mostly invisible to the user, with machine-to-machine negotiation hidden behind the scenes. Credit card companies have been doing this for years – fraud detection that is invisible to the user that successfully detects crime without friction for the consumer.

Machine-learning and artificial intelligence will be utilised to pull insight from authentication events and find behavioural patterns.

I have hope for a future where authentication is seamless (and mostly invisible), where identities are less hackable, and where passwords are obsolete. Until then, let’s stop blaming the user and focus instead on making authentication technology that doesn’t require us to make a choice between usability and security. ●

Eleanor Dallaway
Editorial director
Infosecurity Magazine

Commercial feature

Thorny underbelly of enterprise authentication

Nearly every enterprise in the world is at risk of a major but stealthy cyber attack that exploits flaws and vulnerabilities in their authentication protocols, and many don’t even know it

Exploitation of privilege and authentication is evident in nearly every major ransomware attack or data breach, costing hundreds of millions of pounds in business disruption and reputational damage. These attacks have been on the rise for years and continue to grow at pace, and yet most organisations are not prepared.

Attacks on Kerberos, the default authentication protocol for domain-controlled devices on Windows, are particularly common among cybersecurity incidents. Attackers will frequently leverage limitations in Kerberos and Microsoft Active Directory, the underlying application that supports who can do what to whom on most enterprise networks, to forge false Kerberos tickets capable of granting them administrative privileges.

Detection of these forgeries in post-attack forensic analyses is often impossible because standard logging of enterprise domain controllers and Active Directory doesn’t see or capture the necessary data.

This is a vast problem considering nearly all the world’s large corporations, including 95 per cent of Fortune 500 companies, run on Active Directory. All enterprise security is premised on authentication working correctly and that users are who they say they are, yet Kerberos attacks are simple to carry out with open-source tools, such as Mimikatz and Rubeus, which are now freely available on GitHub and allow hackers to impersonate internal users with illegitimate but accepted credentials. All the logs in the system will say it’s a legitimate user taking an action, even when it’s not.

In the current decentralised work environment, where so many employees access resources remotely, addressing authentication is a challenge every business should be prioritising. But it must be done correctly if they are to avoid falling victim to data breaches or ransomware attacks. A company that can’t ensure users are who they say they are will have a hard time knowing the right people are doing the right things on its computing network.

Consequences of not taking appropriate measures to detect and stop attacks against authentication infrastructure can be catastrophic and multi-factor authentication, while helpful elsewhere, is powerless against this phase of the attacks.

“The thorny underbelly of authentication is that every single system in the enterprise, from a security perspective and from a business perspective, assumes you are who you say you are,” says Jason Crabtree, co-founder and chief executive of QOMPLX. “At this point, that’s a really dumb assumption because protocols like NTLM, Kerberos and SAML can all be manipulated to allow hackers to not be who they say they are.

“The only way to catch this is to diligently work to disable legacy protocols like NTLM and buy either Microsoft ATA/ATP or a more comprehensive and effective tool set from QOMPLX for monitoring and validating Kerberos. Only QOMPLX takes the details of every Kerberos interaction and keeps a stateful ledger to track that every presented credential is duly issued and presented in near real time, massively improving detection accuracy.”

QOMPLX can validate every single Kerberos transaction across global enterprises and its attack detection techniques remain valid regardless of which tool is used to forge a ticket. Its cybersecurity decision platform Q:CYBER is the only analytic framework able to detect the most devastating attacks in near real time, without false positives and with high confidence using targeted model-based detections.

“A huge number of organisations are in a position where they have tremendously expensive security programmes that basically don’t matter as they are based on unreliable data,” says Crabtree. “If they aren’t doing this real-time validation of authentication events, then downstream applications and detections can’t operate correctly.

“With five years of tremendous investment and effort, we’re the only company in the world that keeps track of every authentication event in order and at scale. Unless you do that, you don’t know if one of those events is forged. Authentication is security control number one. Everything else can follow. If you get that wrong, it’s very difficult to recover later because everything assumes it must be true. It’s like missing gravity.”

57.97bn

Number of malicious login attempts recorded during the 18-month period between November 2017 and April 2019

67,282

Number of phishing domains targeting enterprises identified between December 2018 and May 2019

Akamai *State of the Internet/Security, Financial Services - Hostile Takeover Attempts* 2020

For more information please visit qomplx.com

QOMPLX:

Mitek

When you know your customer, you can say “yes” more often.

By combining the world’s best forensic experts with the industry’s most advanced technology, only Mitek delivers banking-grade identity verification with the highest possible assurance levels that can reduce fraud and cut costs.

Discover more at MitekSystems.com

A NASDAQ® Company | San Diego | London | Amsterdam | Barcelona | New York | Paris | St. Petersburg

miteksystems.com