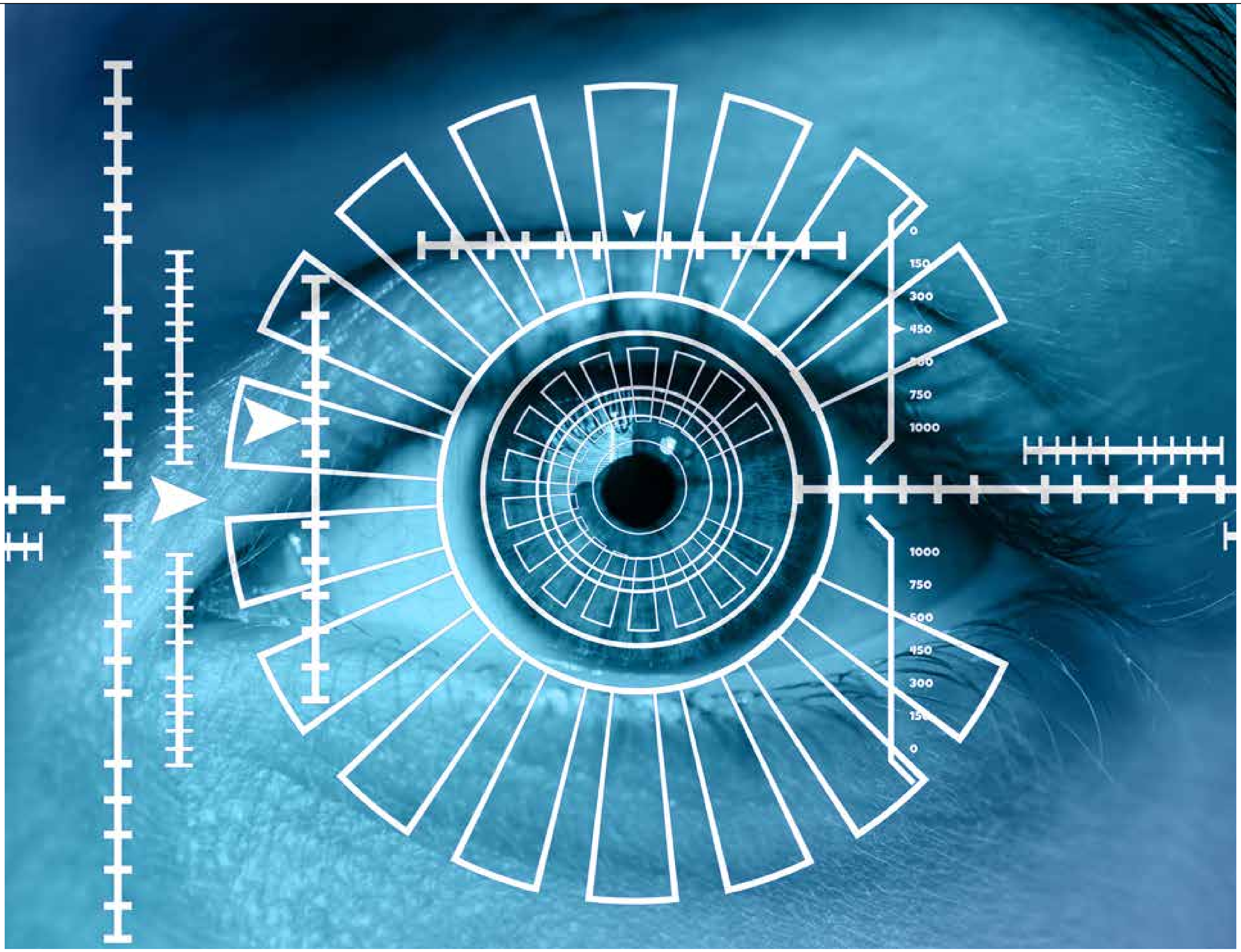
IDENTIFY YOURSELF

Dr Clive Summerfield *reports on the importance of securing customer services and facilitating online education*



Picture credit: Getty

Before the internet, most customer service was delivered face to face. You went to the store and spoke to the shopkeeper one-on-one. Yes, for high-risk transactions such as banking and high-value credit card payments you needed to sign to authorise a transaction, but for the large part customer services were personal. There were no PINs, no passwords, and no one-time access codes. With the evolution of the internet, things changed.

In 2018, it is estimated 1.8-billion people purchased goods online. COVID-19 has only accelerated the trend towards online services, with some estimates putting growth during May (at the height of the pandemic) at 77 percent year-on-year. All online sectors are seeing growth and, while many of us are used to shopping and banking online, COVID-19 has accelerated the transition for sectors such as education, healthcare and Government services.

However, along with this wholesale shift to online services comes the inevitable explosion in online fraud. Fraud was already at epidemic proportions prior to the pandemic, but the past nine months has seen online fraud – and specifically identity fraud – doubling. FTC, for example reports credit card fraud jumping 104 percent in 2020 from levels the previous year.

Similarly, while online identity fraud problem used to be primarily a problem for businesses, the move online exposes our national institutions – such as universities and healthcare providers – to greater risk, not to mention the inconvenience to individuals affected by fraud.

The Unisys Security Index, a publication now in its 20th-year, tracks people's security concerns. It still ranks online fraud and identity theft as the top security threats. This is consistent across all developed and developing economies and even outranks the threat from a pandemic during a pandemic!

The threat of identity theft and fraud has not gone unnoticed by regulators. They have pushed through increasingly stringent identity authentication and data protection requirements to stamp out the most serious consequences of identity theft, including money laundering, terrorism funding and obligations on organisation to protect customer personal information.

But despite all the advances in securing internet communications, proving your identity for access to a secure website still relies on passwords; a primitive and almost universally hated security technology that dates-back to the Sixties.

The average person has 19 passwords, some have more. Trying to remember them all is pretty much impossible. That is why many use the same password for multiple accounts. One in three of these do not meet basic security requirements for complexity and many recycle their passwords, resetting passwords back to one that has already been compromised.

To address the problem of remembering all those passwords, browsers do store passwords, allowing a user direct access to secure websites, such as shopping, social media, emails and so on without them having to explicitly enter a password (if you wish). While this has enhanced the user experience, it does mean that anyone with access to your computer has access to your online services.

Biometrics, technologies that utilise physical and/or behavioral characteristics unique to an individual have long been vaulted as a solution to the password problem. The best-known biometrics – fingerprints, face recognition and voice biometrics – have all found application in access control and telephone security, but have not been widely adopted for internet security.

For example, fingerprint sensors have been used for many years for physical security, such as access to premises and time and attendance in workforce management. But fingerprint biometrics only really came of age in 2013 when Apple introduced Touch ID to unlock smartphones and then when it expanded it to unlock Apps Store and Payment applications a year later. Some banks use the fingerprint to secure online mobile transactions, but these are the exception and the technology is a long way from being used as a universal authentication technology for secure online services.

FARX ONLY VALIDATES SPOKEN COMMANDS WHEN THE USER IS ADDRESSING THE WEBSITE

Similarly, face recognition has been widely adopted in passports and border control. Recent developments have also seen face biometrics appear in some IT security and online identity authentication applications, but the applications are far from universal.

In the telephone customer service, voice biometrics is becoming more prevalent. Many banks in the UK, Australia, Canada and New Zealand, along with some Government agencies, have adopted voice biometrics for automatic call identity authentication.

The best-known biometrics have not been widely adopted for internet security

In telephone services, voice biometrics has a strong business case as it eliminates the need for customers to answer personal information questions (such as mother's maiden name) which not only speeds up the service delivery saving the business money, but is far more accurate and a highly effective tool to detect and track and identity fraud in the telephone channel.

While biometrics are proven as a powerful identity authentication technology for specific applications such as access to devices, border control and telephone call centres, the wide spread use of biometrics has yet to be maximised as a technology to secure online services and applications.

Supported by technology accelerator BetaDen, Voice Biometrics Limited based in Malvern, Worcestershire has been working on a new paradigm for online identity authentication. Code named FARx, it is a piece of website technology that provides seamless continuous verification of the customer's identity while browsing a secure website, such as banking, retail, social media, healthcare, education and so on.

The concept is simple. On accessing a FARx enabled website, the FARx code downloads to the browser on the user's device, be it PC, laptop, tablet or smartphone, and switches on the camera and microphone on that device. Naturally, these are only switched on with the user's permission. This in effect allows the website to see and hear the user accessing the website, much like a familiar video conference call, but now with a website.

Behind the scenes, FARx utilises a unique combination of biometric and non-biometric technologies to continuously track and validate the user's identity. Fused speaker and speech recognition technologies recognise who the speaker is and what they are saying. This works

▶

in tandem with face biometrics to validate that the voice matches the face. After all, voices come from faces and the right voice must come from the right face. To enhance privacy, 'gaze technology' analyses eye movement to ensure that the voice is only monitored when the user is looking at the camera and speaking to the website. This is unlike many voice-only technologies that have to continuously record and listen out for key words in order to respond. By contrast, FARx ignores the speaker if their face is turned away. It only recognises and validates the user's spoken commands when they are addressing the website.

Depending on business rules, FARx also can blank the screen unless the verified face is detected. Rules can also be applied that blank the screen if multiple faces appear. This is useful when accessing confidential information from an insecure location, such as viewing medical records, financial reports or Government information from your home office or a public place.

> THE PAST NINE MONTHS HAS SEEN ONLINE FRAUD – SPECIFICALLY IDENTITY FRAUD – DOUBLING

The experience is much like video conferences, such as Zoom and WebEx, which people have become more familiar and comfortable with over recent months. But instead of interacting with another human, FARx interacts with a biometric engine that is informing the secure website of the identity verification status of the person accessing that website.

Authentication can be continuous or intermittent depending on the business requirements so, for example, for delivery of confidential health services, you may want continuous verification but if it is a simple payment service, momentary verification is probably all that is needed.

The big benefit of this approach is that it is incredibly cost effective. It uses existing browser technology and hardware on the user's device. There is no need to provide additional biometric hardware or software. No need to rely on the person having a separate mobile phone (and mobile connectivity) for SMS one-time passwords. Or for that matter, no need to rely on the customer having access to email. The authentication process remains inside the browser and is protected by the same security and encryption protocols that protect the browser session.

While originally developed with online banking and financial services in mind, the COVID-19 pandemic has driven significant interest in FARx from the education sector. COVID-19 has caused many large educational institutions to accelerate the transition to online delivery of educational services. This has highlighted the issue of student identity and specifically the identity of students during online examination and testing. How do you know that it is the registered student taking the online examination?

Working with suppliers of online solutions to leading universities around the world, Voice Biometrics Limited has been developing FARx to allow continuous authentication of students undertaking online examinations.

Using the camera and microphone on their computer, FARx detects if the correct face is in front of the computer and blanks the screen when there is no face, the incorrect face or when multiple faces are detected. Voice biometrics augments the face recognition to positively assert the student identity and to detect if the student is speaking during the examination.

The FARx concept is in its infancy. The next stages involve marrying FARx with AI chat bots, speech synthesis and avatar technology to provide a secure two-way multimedia conversational user experience. In effect, this creates a synthetic customer service agent that recognises who you are, what you want and responds using spoken and visual cues. A very different paradigm to current PINs and passwords and much more like the face-to-face customer service experience that pre-dates the internet ●

Dr Clive Summerfield is founder of Voice Biometrics. He has over 30 years' experience developing, implementing and deploying voice biometrics and speech recognition into a wide range of markets and applications.

Voice biometrics is becoming more common in the telephone customer service

Picture credit: Getty