Cyber Security

Best of Money: hacking into your account is easier than you think

Fake fingerprints, selfie masks and voice tapping mean the wealthy should be worried

© James Minchall

Martin Arnold and Hugo Greenhalgh NOVEMBER 4 2016

Anyone who has ever struggled to remember the password for their banking app or fumbled with a card-reading device can appreciate the sheer joy of using their fingerprint, voice or face to access their bank account quickly via their smartphone.

Most big high street lenders now use the latest biometric technology to give customers a more convenient way to check their account balance or make payments. However, one big question remains unanswered: is it safe?

A cyber security expert from consultancy NCC recently visited the Financial Times to give a demonstration of how to hack into a smartphone's biometric authentication software.

Matt Lewis, NCC research director, showed how to make a copy of his own fingerprint using wood glue, candle wax and a printed circuit board that allowed your correspondent to hack into his smartphone.

He also tricked voice-recognition software by playing back recordings of his own voice and produced a 3D-printed mask of his face based on photos of himself, which was then worn by your correspondent to hack into his phone.

While you cannot forget your voice or face — making them a simpler way to check your identity — they are also much harder to change than your password if they are ever stolen by cybercriminals. This means that if biometrics becomes the dominant form of authentication it is likely to be much more damaging if the systems are hacked.

As more financial service providers launch new biometric identity-checking schemes — such as MasterCard's so-called "selfie pay" service that lets people make mobile payments by photographing themselves, Wells Fargo's eye vein scanning system, or HSBC's Voice ID — experts say security will become a more pressing issue.

"Biometrics aren't the same as passwords — they aren't secret," says Mr Lewis, a former technology specialist at GCHQ, the government's electronic intelligence agency. "You need other elements to ensure fraud is prevented. If a database of fingerprints is hacked into, that could compound the problem."

Batten the hatches

Cyber security has already shot to the top of the boardroom agenda for banks, particularly after 76m customers at JPMorgan Chase, the biggest US bank, were shocked to learn that some of their personal data were stolen two years ago.

The seriousness of this threat was underpinned when one of the biggest bank robberies in history was carried out by cyber thieves in an audacious raid on the Bangladesh central bank in February. The crooks made off with $81m that was on deposit at the US Federal Reserve.

FT banking editor Martin Arnold tries on a face mask in a demonstration of how biometrics authentication could be hacked

“It is a very intimate game between organised crime innovating attack methods and the banks coming up with defences against these,” says David Ferbrache, technical director at KPMG and former head of cyber and space for the UK ministry of defence.

He reckons that organised crime groups are making so much money from hacking traditional password-based bank systems, that for now they will be in no rush to switch their attention to the challenge of cracking biometric controls. “But over time they will start to spend more time looking at biometric identity.”

Most UK banks already allow customers to logon to their accounts using their smartphone’s fingerprint reader. This has the advantage of keeping the biometric data on the phone, rather than stored centrally by the bank on a database that could become a target for hackers.

Robert Capps at NuData, which tracks people’s behaviour through their phone to authenticate them, says most biometric checks are no safer than a traditional password. If hackers gain access to your password, they can set up a new mobile account pretending to be you. “It all comes down to the enrolment process — and that is back to the username and password,” he says. “This is not the great panacea.”

Voicing the issue

Several big financial institutions are now focusing on voice-recognition systems to identify their customers. Unlike phone-based fingerprint scans, these typically involve a customer’s digital “voiceprint” being stored by a bank and used to verify who they are when they call.

Voice biometrics has a long history. The concept can be traced back to Alexander Melville Bell, father of Alexander Graham, who in 1867 published a book called *Visible Speech, The Science Of Universal Alphabetics: Or Self-Interpreting Physiological Letters*. Bell’s notion was to focus not so much on the spoken word, but on how they are being said.

Further developments by Russia and the US saw voice biometrics gain greater traction — and accuracy — in the 1970s and 1980s, but a series of false starts meant that the technology has not been widely adopted until today.

Now it is set to become big business — and not just for the banks. Research by Tractica, the market intelligence firm, suggests that revenues from voice biometrics could top $5bn by 2024, up from just $245m in 2015. It sees the greatest adoption among consumers using their mobile phones, as well as benefits for call centres and healthcare providers.

Other banks, such as Capital One, are using voice technology to enhance their services: its customers can now check balances and pay off credit card bills by speaking to Alexa, Amazon's voice assistant, which sits on voice command devices such as Echo.

But the telephone is also a popular medium for fraudsters. According to Financial Fraud Action UK, British consumers and financial institutions lost more than £750m over the course of last year — a jump of 26 per cent from 2014. Telephone banking fraud almost doubled over the same period, up by 92 per cent to £32.3m.

One out of every 2,500 calls to call centres run by banks and other financial services companies is fraudulent, data from Infiniti Research recently revealed.

How it works

The technology has improved greatly in recent years. Gone are the frustrations of repeatedly saying "yes" or "no" into an automated system that cannot understand your accent. Today's programmes can determine who is speaking as well as working out what they're saying.

There are nonetheless different technical approaches. Lloyds has just agreed a deal with Pindrop, a voice fraud prevention and authentication company, to offer what the tech firm calls "phoneprinting" to its 30m customers from the beginning of December.

This is not technically biometrics, but works in a similar fashion. The customer makes a call, and the programme analyses 147 different call features that range from the type of phone you're using to the type of background noise. "It adds a layered picture — everything outside the voice," explains Matt Peachey of Pindrop.

The key function is to deter phone fraud and improve customer security by highlighting unusual activity. Lloyds intends to take a further step and introduce full voice biometrics by the summer of 2017.

HSBC has opted for technology that cross checks 100 unique characteristics of a person's voice — including speed of delivery, natural cadence or pronunciation — as well as certain physical aspects that listeners cannot discern, such as the shape of the customer's larynx or their nasal tracts.

"The technology measures the way your muscles produce the sound rather than just the sound itself," explains Francesca McDonagh, head of retail banking and wealth management at HSBC. "It will then record a voice print — my voice is my password."

It is a development that will be welcomed by those burdened with many online accounts and an array of passwords. But concerns have been raised over whether customers will be comfortable divulging this level of information. Will they really be happy for their bank to know the shape of their larynx?

"The key perceived disadvantage for customers relates to privacy," says Anthony Duffy, UK director of retail banking at Fujitsu. "Some individuals are not comfortable with organisations — particularly large companies — holding biometric data.

If the “nightmare scenario” is that a large depository of biometric data — such as fingerprints — could be stolen, something approaching this has already happened: last year, hackers stole 5.6m sets of fingerprints from the US Office of Personnel Management, which oversees civil servants in the federal government.

“If a customer is logging on to check their balance face-recognition may be enough, but for a high value transfer they may say it has to be multi-touch identification where both fingerprint and face are required,” says George Avetisov of Hypr, a biometric data encryption company.

André Malinowski, head of international business at Computop, says biometrics will never be watertight and customers should always insist on a secondary ID measure, such as an old-school password or Pin. “[With biometrics] we are talking about something you cannot change. And if it is compromised, it is compromised.”

© Getty

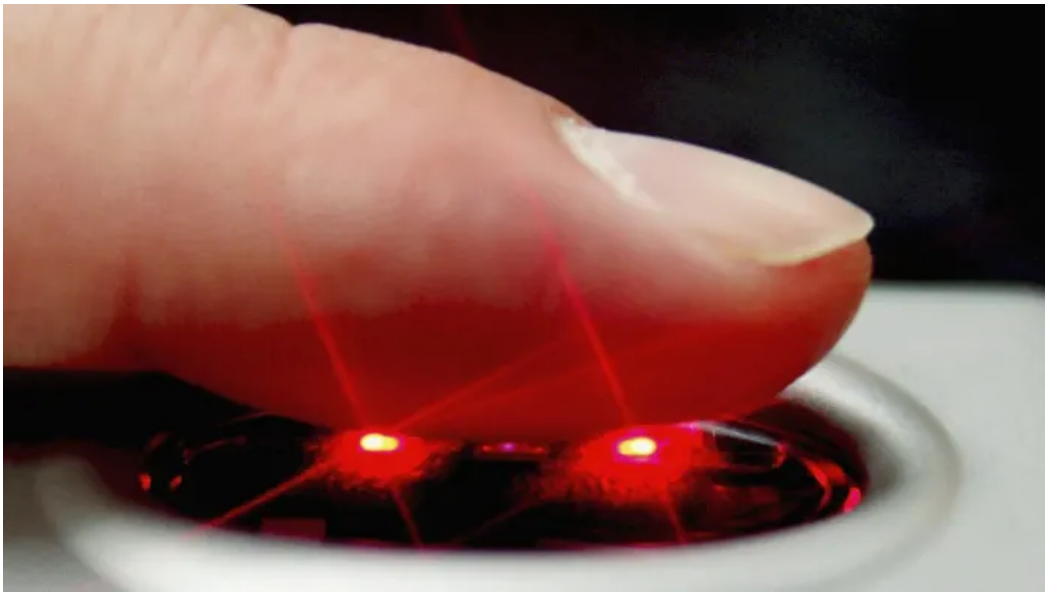
Behavioural systems

Ultimately, making mobile banking truly convenient while reassuringly secure is likely to rely on even more sophisticated systems that use hundreds of different data points — from how fast we type to where we are — to build up a unique profile that can be used to recognise us automatically whenever we use our phone.

These behavioural biometric systems are already being piloted by several banks and have the advantage of being much harder to fake while also not being usable across multiple accounts of the same person. “Wind the clock forward five years and you will see a combination of behavioural biometrics and quite sophisticated analytics and risk -scoring on each transaction,” says Mr Ferbrache at KPMG.

If they can crack the security problem once and for all, the potential for savings by the banks and other financial services providers is huge. For example, MasterCard, the payments processor, has spent $1bn on security over the past three years alone. “More than 50 per cent of the global fraud in our ecommerce business is digital,” explains Ajay Bhalia, MasterCard president of global enterprise risk and security.

With more than 2bn cardholders, MasterCard is ramping up its defences against possible fraud, investing in voice technology, but also looking into security measures based on fingerprints, facial recognition, heartbeat technology, eye veins and irises. It is running a pilot scheme with ABN Amro in the Netherlands and is now looking to roll it out to 12 European markets, including the UK, in early 2017.



The hassle factor

In strengthening the barriers to fraud, though, banks and card providers are exercising an unspoken trade-off between efficiency and security. Customers become frustrated if it takes too long to go through the authentication process; banks then lose custom as people just put the phone down.

Yet given how time-consuming most biometric hacking techniques appear to be — such as copying someone’s fingerprint or making a mask from their photo — some experts believe they are likely only to be worth doing for targeted attacks on wealthy people.

Most banks and financial institutions will retain several hurdles for wealthier customers to clear before allowing them access to their accounts. It may be more hassle, but again if it’s a question of ensuring fraudsters do not have access to your money, it is a price many will be willing to pay.

“When it comes to protecting consumers from cyber threats, the greatest challenge is balancing security with convenience,” says Keiron Shepherd, senior security specialist at F5 Networks. “However, these often lie down divergent paths. Like all things in security, voice biometrics is not the silver bullet, but another tool to defend against cyber criminals.”

The accent is on identity checking

What happens if my voice changes? Or I have a strong regional accent?

Siri, an automated voice recognition personal assistant introduced by Apple on its iPhone 4S back in 2011, struggled at first with regional accents. Tabloid journalists gleefully reported that one particularly salty Scottish phrase was repeated by Siri as “Eurobond bank” — not quite the intention of the speaker.

But voice recognition services — and indeed Siri — have improved immeasurably. Biometrics now covers more than just the spoken word; it delves deeper into how these words are articulated.

“There have also been historic concerns that voice biometrics might be undermined by factors such as regional accents, background noise or people having colds,” says Anthony Duffy, UK director of retail banking at Fujitsu. “However, the latest iterations of such software make such concerns redundant.”

Indeed, the majority of them gauge factors such as the shape of your voice box and respiratory tract; they look at inflection and intonation; and take into account your accent.

“It’s a potpourri of factors,” says Bruce Bomphrey, sales and business development director at Soitron UK.

This means it will take account of regional accents — and learn the way in which you speak. And if you have a heavy cold, it will compensate for those factors, by matching variables other than intonation, for example.

Research is currently being conducted on whether this holds true for another group: those undergoing — or having completed — the process of transitioning from female to male or vice versa.

“It’s a question of whether [transitioning] could affect the fundamental aspects of the voice,” says Dominic Watts, senior lecturer in forensic speech science at the University of York. “The length of the vocal tract shouldn’t change, but I suppose the difference could be if somebody was seeking to develop a lower- or higher-pitched voice. That may raise or lower the larynx and could raise the pitch as well.”

But while that might affect whether the voice recognition software works, the solution is simple: just re-record your voice password.