
Fidelity™
INTERNATIONAL
Digital keys
Passwords, passkeys and the
future of securing your identity.

Unlocking the door to your security.

It's a pretty safe bet that everyone reading this will have used one or more passwords in the past 24 hours. They are the keys we use to lock and unlock our personal and business accounts a dozen times a day, but how secure are they really?

These days it's necessary to create a password to do just about anything online, from internet banking to checking your mail. And, although using and memorising a few short, simple passwords is so much easier than creating several unique, complex ones, many of us still compromise our online security by taking a 'least-effort' approach. In order to protect ourselves, our data and our privacy we need to learn how to craft passwords that are long, strong, and difficult for someone else to guess, while still being easy to remember.

Fidelity™ INTERNATIONAL

The keys to your online life.

These days we all have two sets of keys, the ones we keep in our pockets, that open our homes and vehicles, and the ones we keep in our heads, which unlock access to our communications, banking, social-media feeds, online shopping accounts, work services and so much more. Billions of us use digital and online services like these every hour and it is crucial that there are systems in place to prevent users from accessing each other's information. To achieve this, websites and applications need a way of identifying each of us as unique individuals, with separate, protected access to only our own accounts and services. The most common way of preventing two users from being confused with each other is by getting you to *identify* yourself (with, for instance, an email address or user-name) and then *authenticate* your identity through a singular password or passcode. No prizes for guessing, this simple process is known as *identification and authentication*.

In terms of authentication, having a strong password is one of the first and best ways you can protect your accounts and personal information from hackers and identity theft. Of course saying that is easy, the hard truth is that any decent password must accomplish two quite incompatible objectives; it needs to be long and complicated enough that it's essentially impossible to guess, while also being clear and memorable enough that it can be recalled easily.

You may well have noticed how difficult that particular problem can be. Remembering convoluted strings of random letters, special characters and punctuation is hard, and that's one of the reasons there is a gradual, but steady, move away from passwords, and toward alternative identification and authentication methods (see the **The future of identification and authentication** chapter later in this booklet).

Nevertheless, it is the aim of this document to provide you with the ideas and techniques you'll need to make the best, strongest, most individual passwords, passcodes and PINs (Personal Identifier Numbers) you possibly can, to help ensure that the only person with access to your entire online world, and everything that's in it, is you.

Fidelity INTERNATIONAL

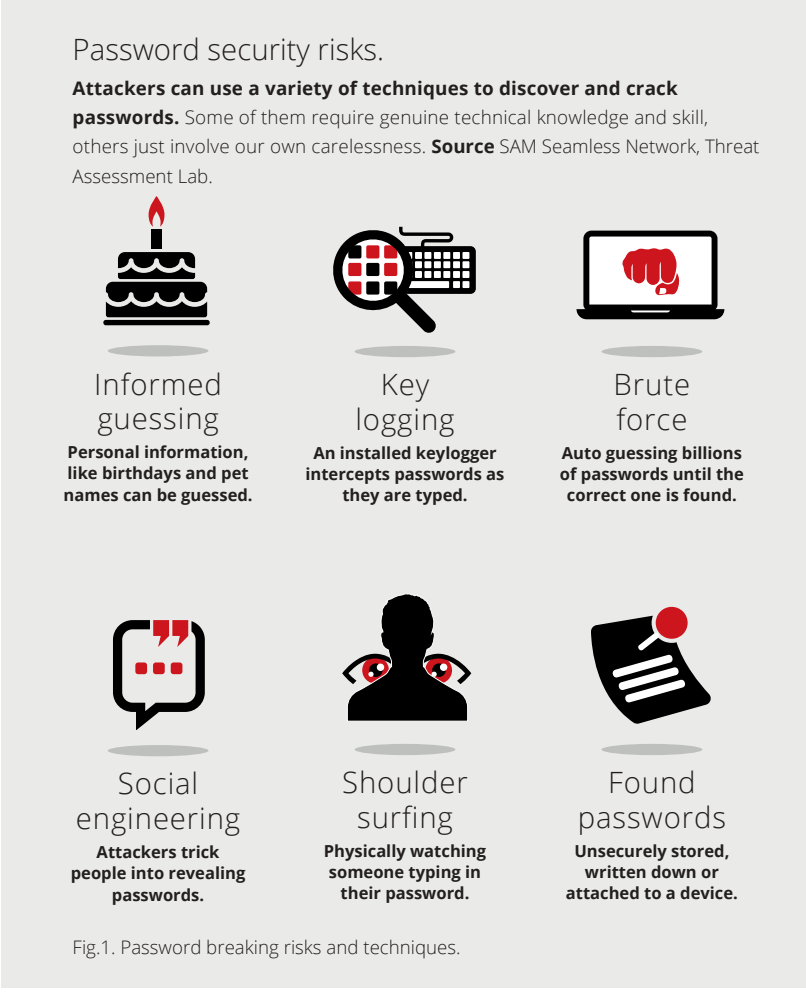


Fig.1. Password breaking risks and techniques.

Password vulnerabilities and risks.

Beyond the self-evident methods attackers can use to steal your passwords, codes, PINs and security numbers; like looking over your shoulder when you're using an ATM, or trying to overhear you if you read out your card details over the phone, there are a number of more advanced methods available to those with a little knowledge. Bear with us here, because knowing what they are will help you understand why a weak choice of password could leave you vulnerable.

'Brute-force' attacks.

When hackers are trying to crack your password there are a couple of different methods they typically use. The first is called a *brute-force attack*. This involves a piece of software working tirelessly through all the possible variations and configurations of characters, numbers and symbols on a keyboard. Starting with 'a' through to 'z' and then 'aA' to 'zZ' etc, entering each in turn with the hope of eventually inputting the correct value. Programs using brute-force attacks can make anything from 10,000 to 1 billion guesses per second, making this method very fast when used to break shorter (6 characters or less) passwords. Longer, more complex passwords have many more possible values making them exponentially more difficult to crack. To have a chance of breaking them in the hackers own lifetime (*see fig.2*) they need to move on to the next method.

Dictionary attacks.

This entails a computer program trying entry after entry from a particular reference work or database to access your account. These 'dictionaries' don't have to be the usual A-Z variety, they can consist of anything; lists of commonly used and previously cracked passwords, names of celebrities, historical figures, significant dates, and so on. In a dictionary attack a computer tries one log-in attempt for each 'dictionary' entry and, if that one fails, it just moves on to the next. All at lightning speed.

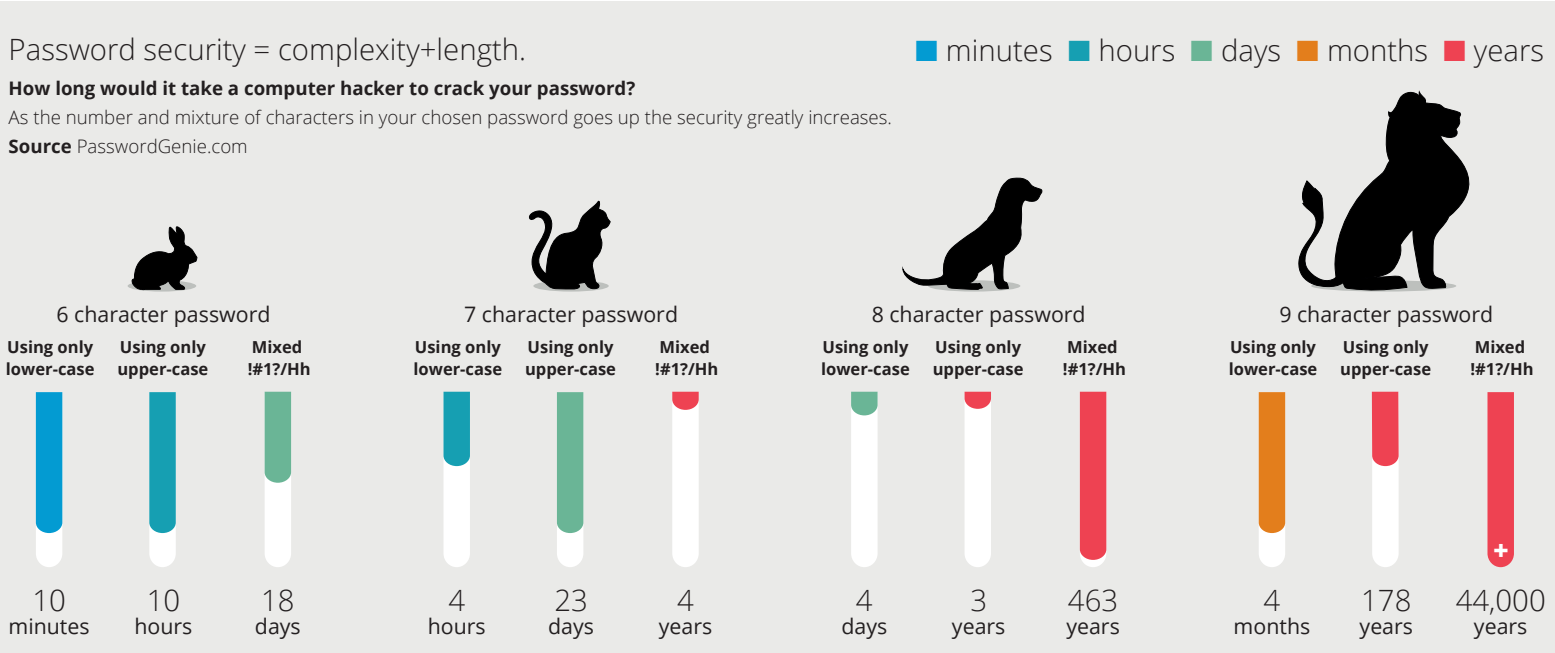


Fig.2. Password length Vs time to break..

Fortunately, most computer systems have a pre-defined limit on the number of unsuccessful login attempts which can be made before an account is locked and requires an administrator's intervention to reactivate. The security of your password on any given site, service or application, depends entirely on how your credentials are being stored (and how seriously the site, service or application takes it's security). There are some sites that will store your log-in credentials in simple, easy to read text - exactly as it appears when entered by you. So if your password was, for example, *Sa77yjon3TonE's3EY* (SallyJonstone'sKey) that's exactly how it would be stored in the companies database, as: *Sa77yjon3TonE's3EY*. Known as 'plain text' it represents the lowest possible security you can afford to a password. This means that if a hacker gains access to the database containing your password it doesn't matter how long or complex you have struggled to make it, your password could be read as easily as you are reading this sentence now. To increase

safety many sites will go significantly further to protect your private log-in credentials by taking that plain-text and mixing it up, using a mathematical process known as '*hashing*'.

Password 'hashing'.

Hashing a password means turning it into a scrambled representation of itself. By using a secret key the site makes what is called a 'hash-value' which uses an algorithm to make a unique code. The final hash-value bears no resemblance to your original password. So, for instance, the hash-value of *S!vSPu55_0rX* might be: *20c9ad97c081d63397d*, and changing just one character or number of your password will result in a completely different hash-value output.

It's an example of what is known as a 'one-way function'. This means that there is just no way for someone without the key to work out what the original password was. If a hacker were to access the password database, as long as they were translated into hash-values, there isn't any way for them to use that information to access your account. They would just see strings of 'hashed' numbers and letters instead of plain-text passwords.

Hackers can't enter hash-values into the 'enter password here' fields nor can they 'translate' the hash-values back into plain text to reveal your password.

Staying secure means being aware.

You may well think, OK, that's all fine then. Regrettably, while you can't turn a scrambled hashed-value directly into a password, for hackers there is a work-around. How they can discover your true password is what we'd like to discuss next. And it's important for you to understand because, by following our advice, you will be able to foil even the most capable of criminals.

The worst of the worst, how NOT to write a password.

NordPass.com trawled through over 500 million passwords which had been leaked as a result of data breaches in 2019. The following results and statistics highlight the most common shockingly insecure, weak (and sadly predictable) passwords and behaviours. Below you can see the top ten most used passwords (out of 500 million) and some percentage breakdowns of the typical make-ups of those passwords. **Source** NordPass.com

Fig.3. Worst passwords and behaviour from 500 million+ accounts.

With access to a database of hash-values criminals can use a variety of techniques to find the key; by using a *brute-force* or *dictionary attack* (see above) they can generate *their own* hashes from strings of words, characters, numbers and symbols. Using software which can throw thousands of attempts a second at the problem until it finds a value that exactly matches the hash-values on the stolen list. And then, of course, they have your log-in details.

The good news is that the longer your password, the longer a brute-force or dictionary attack is going to take to crack it. And the longer the attack required, the more time-consuming and expensive it will be to match the hash-value and discover the password. But it's not just length which is important. As most people make their passwords up out of normal words, attackers will almost always start checking hash-values with dictionary words first. This makes the *configuration* and *complexity* of your credentials vital.

Making great passwords.

As we've seen, because these attacks use stores of dictionaries, encyclopaedias and word-lists to power their guesses, a really random password will be much more much secure than one made out of a standard-issue dictionary word. You can see just how much of a difference adding unusual characters and numbers makes to the security of your password by reading *Figure.2 - password length Vs time to break*.

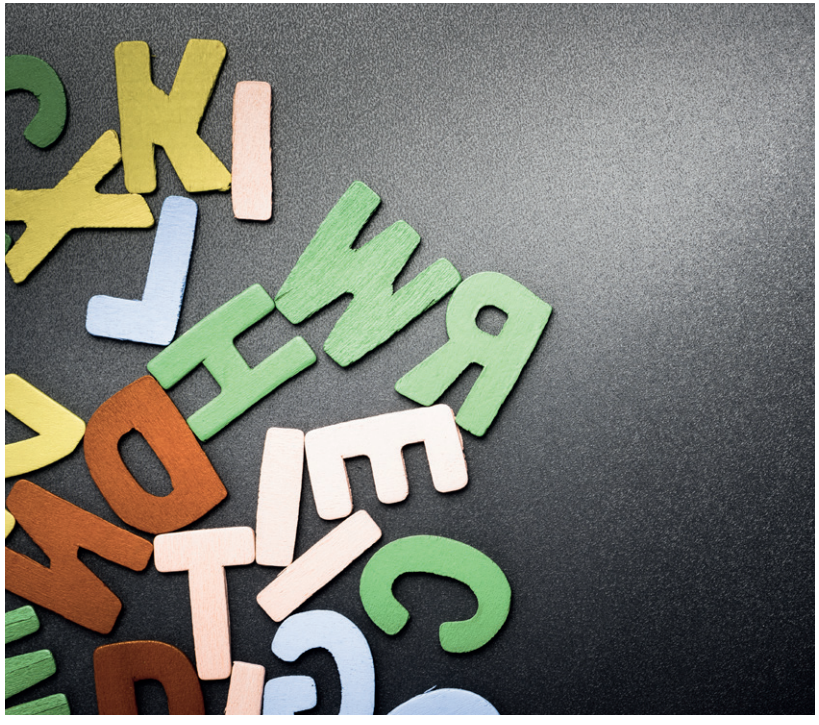
While thinking of an entirely unconnected sequence of characters might make for a very secure password it would also be almost impossible for most people to memorise. Probably the best way to craft secure, long passwords made up of a collection of numbers, letters and symbols, that doesn't resemble a dictionary word, but is possible to remember, is by taking a few random words and making a memorable 'phrase', and then converting it using a few simple techniques into something long, mixed-up and strong.

Passphrases.

A common approach is to choose a popular, pre-existing phrase; a snatch of song lyrics, a line from a favourite film or novel or a famous quote, and simply capitalise some letters at the start and finish, change a few 'E's to '3's and add an exclamation point to the end. While this might strike you as pretty much unguessable you would be underestimating the capabilities of the people and software dedicated to cracking your code.

Don't forget, hackers have databases containing the scripts of every film and television show ever made, the lyrics from every song ever written, the text of every book ever digitized and every page in every language on Wikipedia. Can you be sure your passphrase would survive that level of scrutiny with just a few simple character transpositions?

A much better approach is to take three or more **completely unrelated words** and put them together in no logical order. Here are three words we generated randomly on a website: ***unhappy - melon - athlete***. Let's put them together, which gets us to **unhappymelonathlete** - that's already 19 characters, which is great. Now, as there are three words, let's capitalise the third word, which should be easy enough to remember: **unhappyMELONathlete**.



So far so good. Finally we need some numbers and 'specials' in there. As the **melon** seems to be **unhappy** why don't we give it one of those sad-face keyboard symbols, like this: **:(**

Let's also say our **athlete** came third in a race, we can put a 3 after their name, but we're still really proud of them so lets give them a star * too. So our final passphrase is: **unhappy:(MELONathlete3***.

There you have it, a 23 character passphrase which should be pretty memorable and would, according to *www.my1login.com* take approximately **64 million years to break!** It's not hard to make passphrases like this and once you are used to doing it, it will become second-nature.

Better passwords, a checklist.

Here is a run-through of some of our top advice on making the best, and avoiding the worst, when you are designing your own passphrases, passwords and digital keys.

- ✔ Never use short, simple easy to guess or discover words, like the names of friends, family or pets. Equally, don't use words straight from the dictionary or lazy, commonly used passwords like 12345 or PASSword.
- ✔ Have a different password for every account. There are a huge number of cases of hacking every year that take place because a users' password had been compromised on a low-security website and that user has recycled the same password for another, higher-security site. An attacker either discovers or guesses the associated user-name on the second site and simply tries the cracked password on it.
- ✔ For memorable passwords use a string of unrelated words and sprinkle a mix of upper-case and lower-case characters, numbers and special symbols into them. Try to make where you put them and what you use memorable, like we did in our example, without just substituting '1's for 'L's.
- ✔ Don't ever share your passwords with anyone, for any reason, and don't leave passwords written down and lying around on sticky notes attached to your computer, on notebooks you leave on your desk or in computer files.
- ✔ Before you trust a site by entering your password (or any log-in details) make sure you have a secure connection by checking that the site's address in the browser window begins with: **https**://. This means that the site is using a secure link that should be safe from interception.

Top five best and worst practices.

Here are our top five tips for creating good, strong passwords, and our top five practices to avoid at all costs.

Do

Use a good mix of upper and lower-case characters, numbers, symbols and punctuation.

Add in made-up and invented words which are not in any dictionary.

Use a 'pass-phrase' by putting three or more random words together and mixing them up.

Make sure no one can 'oversee' you as you are entering your password or passcode.

Create a brand-new password each time, don't just change one character on the old one!

Don't

Create a password which is less than eight characters long. Aim for twelve or above.

Repeat previously used passwords or re-use passwords from other accounts.

Use a birthday, favourite sports team or anything personal that could be discovered online.

Write down your password and store it on, near or with your computer or device.

Use patterns of letters or numbers to make your passcodes or passwords.

Password management.

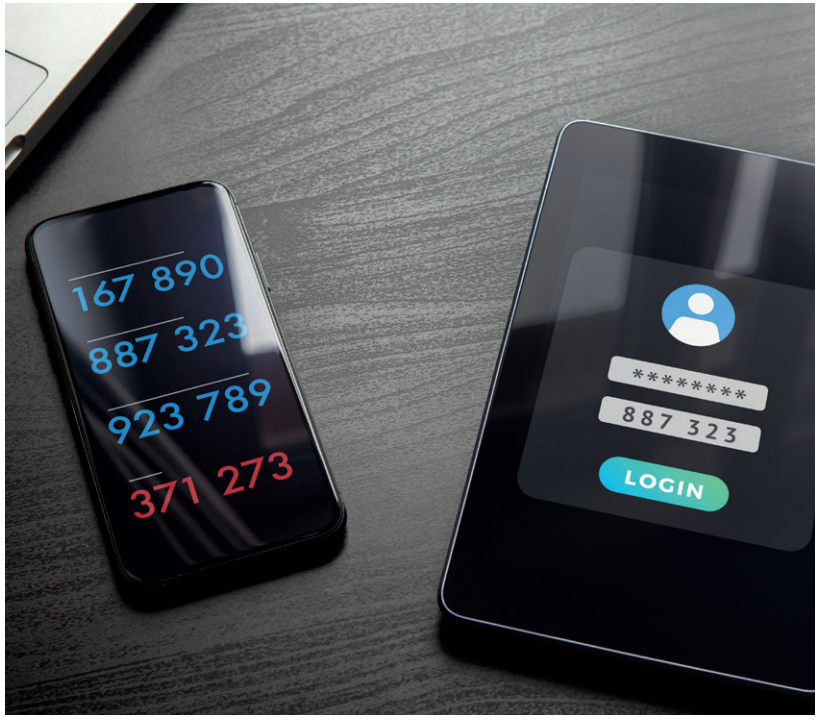
While, as we have seen, it's perfectly possible to design and use highly secure and memorable passwords and passphrases it can be difficult when you need to remember several of them for all the different accounts you need to access. If you're having trouble keeping so many in your head then consider using a *password manager*.

A password manager is an application or program that runs on your computer and can not only store your own passwords, codes and passphrases but generate new, very long, highly complex ones for you, and retrieve them as necessary. Some of the more sophisticated versions include browser plug-ins which allow you to log-in to a web page with a single click. They are also handy for auto-filling forms, and syncing-data across operating systems and devices.

Think of them as an encrypted digital vault, and, as such, consider our advice below and spend some time researching which version you think would best suit your needs. There are plenty of free ones out there, but you may feel your security is something important enough to spend a little money on.

As password managers contain the most valuable information about your online identity, before you decide on a particular model you should check that it, itself, requires a password to access it. If it doesn't then anyone who can gain entry to your device would have your whole rota of log-in details.

Similarly, the passwords held on the manager itself need to be encrypted for maximum security. Regrettably hackers have occasionally managed to find ways of successfully attacking password managers so it's vital that you install any security updates and keep operating software up-to-date.



Many web browsers and operating systems (like Apple's iCloud Keychain and the Credential Manager in Windows 10) will offer you the option of remembering passwords when you enter them into website log-ins. This kind of password management can be very convenient for accessing your most frequently used secure sites (shopping, banking and so on) but you need to be very careful if you use them on any computer or device that you share with other people.

Adding an extra layer of security.

Sometimes online accounts will ask you for information other than your password, things like your date of birth or home address. If it's an official site, like your online banking account, your responses should be accurate, but for other sites which require 'memorable information' (commonly used to re-set your password if you have forgotten your log-in credentials) consider inventing your answers. This will afford you an extra layer of security by ensuring that anyone who accesses public information about you, from social media pages for instance, won't be able to use the fact that they've discovered your pet's name, or the first school you used to attend, to answer your security questions.

The future of identification and authentication.

Most security experts agree; we're not likely to experience the death of the password anytime soon. But, as we have already seen, they're far from ideal so what could the future of Identity and Access Management (IAM) hold?

Multi-factor authentication.

Multi-factor authentication works by adding an additional element to the log-in process. This requires two or more pieces of information (like a password and a one-time code sent by SMS) for successful entry to an account. If a company, application, website or service offers multi-factor authentication, you should definitely use it.

This security method has actually been available for some time. When, for instance, you use an ATM to withdraw money you are using a very effective and common example of a two-factor authentication process. The first factor is your bank card, which you place inside the machine, and the second is your personal identification number (PIN) which you then input. Having just one of these components alone would not be enough to access your funds.

Moving beyond simple passwords.

Many experts believe the days of the standard passwords are dying out. With the advent of more advanced technology, the future of the keys you use is changing.

Multi-factor authentication

Combines the use of two or more credentials together, eg combining:
Something you know, like a password with something you have, like a phone.

Persona-based authentication

A combination of personal, unique individual elements:
Geographical elements. like location with behavioural elements, like voice patterns.

Trust-score system

Several behavioural elements are combined to assign a 'trust-rating':
Combining your location + facial recognition + your known typing pattern.

Zero-interaction authentication

Users do not need to directly interact with a system to log-in:
A device carried, like a key-fob or thumb drive works as a security key.

Digital-certificate authentication

Digital certificates are granted to a user, allowing access for a set period:
Certificates are delivered via the cloud and are linked to a device.

Biometrics authentication

Verifying your identity by using the unique characteristics of your body:
This includes processes like; fingerprint readers and face recognition.

Fig.4. New ways of authenticating your identity.

Many smartphone manufacturers include a fingerprint sensor in their devices which can be used in a multi-factor authentication process. An example would be a secure log-in process (some internet-banking apps, for instance) which requires a fingerprint, before a pass-code screen requests a PIN to validate your account. Again, the idea here is that if you lose your phone the feature would be unusable without both your fingerprint and code to unlock it. Typically multi-factor processes work by combining:

- Something you **know** (knowledge) like a PIN.
- Something you **have** (possession) like a smartphone.
- Something you **are** (inheritance) like a fingerprint.

The future looks set to add to these such metrics as:

- **Where** you are when trying to obtain access - like at home.
- **When** you are trying to get access - like late at night.
- **What** device you're using - like a tablet.

Biometrics

Biometrics are a way of using the unique individual characteristics of your body to verify your identity. Applying them can unlock a mobile device, book and pay for a taxi-ride or access your bank account, all with a tap of your finger or a spoken word. Biometrics, like fingerprints or voice and facial recognition, are extremely popular among consumers because they are so easy to use, but how secure are they really?

Well, the truth is that the security among devices and manufacturers varies considerably. Apple devices use a 'capacitive fingerprint sensor' in its patented Touch ID system. This uses a finger's natural electrical conductivity to map your prints. By making a digital image of the ridges and folds of your fingerprint, rather than taking a 'photographic' copy of it, Apple claims that there is a 1 in 500,000 chance that someone else's finger will be able to unlock your phone.

Samsung's ultrasonic fingerprint sensor, on the other hand (which works by creating a 3D image of your fingerprint using ultrasonic waves) is often quoted as among the most secure type of biometric device. Recently, however, it was reported that a number of "gel-style" screen protectors may cause the sensor to take an incorrect or 'confused' reading of the users fingerprint, resulting in the phone unlocking itself for *anyone's* fingerprint, not just the owners. With emerging technologies like these, in order to stay protected, you should always stay up-to-date with current security advice and news stories.

Some device manufacturers have recently begun to swap fingerprint sensors for facial recognition technology. Driven, in part, by manufacturer's current preferences for phones whose front is made up of a single full-screen, and which don't, consequently, have space for a dedicated print-sensor.

Face identification software stores a 3D copy (like a living mask) of your face and analyses how shadows reflect onto the lines and planes of your features when light strikes it at various angles. Match enough vectors and you have unlocked the device. With facial recognition it's vital that you use good lighting and a clean camera lens. Face ID software that allows you to enrol a low-quality image will make it much easier for someone else to fool the device into thinking it is you.

Most common passcode patterns.

New data uncovers the surprising predictability of Android lock patterns.
Norwegian University of Science and Technology collected and analysed 4,000 unlocking patterns to reveal the six most-used, and consequently least secure.

Fig.5. Android unlock swipe patterns to avoid.

Passcodes and PINs

The possibility that a criminal would have immediate access to your face, fingerprint or iris is (hopefully!) pretty low. But even if they did, they wouldn't need all your personal biometric data to access your mobile device, all they really need is your passcode. That's why it's so important to be certain that your smartphone or tablets last line of defence is as strong as possible. How can you ensure your PIN or passcode is as secure as it can be?

Recent studies have shown that the majority of people use PINs that express important and significant dates in their lives. Birthdays (of course), your own and your loved ones, and birth-years are the most popular choices. Repeated digits (like 2233) and PINs that are easy to remember and input quickly like 1598 or 2002 are close behind in popularity, so it's critical that you avoid the most common examples. These examples are all four digit codes, and you may well be forgiven for expecting that as the number of digits goes up the code becomes more secure, but strangely that might not in fact be the case.

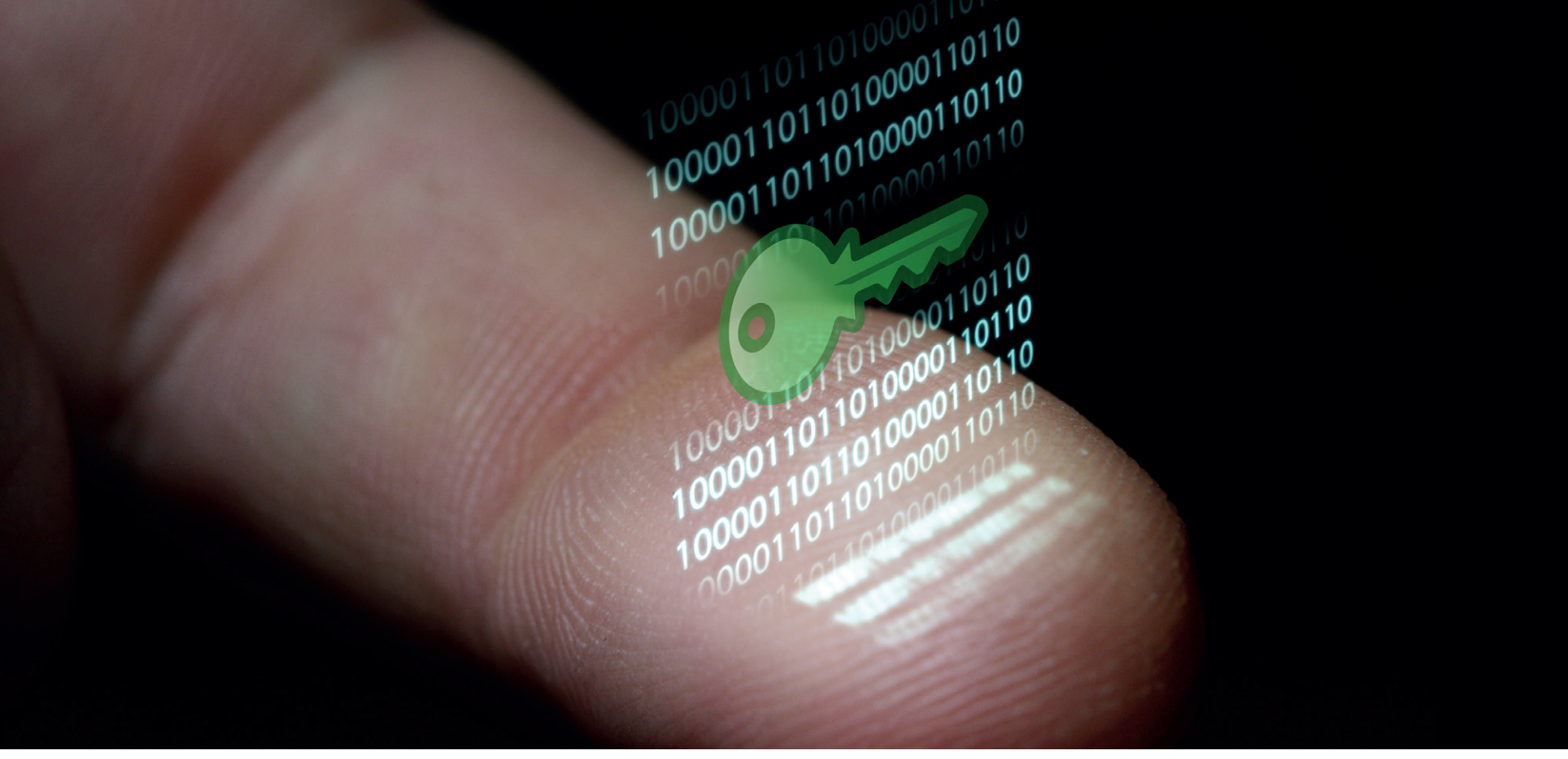
Multi-Digit patterns and swipes.

In order to encourage longer codes some devices allow users to choose an input pattern (or 'swipe') on the keypad instead of entering a sequence of numbers. This can be very fast but may not be very secure. During testing at the *Annual Computer Security Applications Conference*, researchers found that participants who were shown a video of someone entering a pattern to unlock their phone once were able to memorise, and replicate it, 64% of the time. If the video was watched four more times the success rate rose to 80%! So keep your swipes secret, and be on the look-out for anyone 'shoulder-surfing'. Make sure you clean your devices' screen too, a greasy 'swipe-streak mark' would make your pattern obvious.

The final key.

In summing-up; it seems that, in the long run, technologies like palm and fingerprint biometrics, multi-factor authentication and facial recognition software will be rolled out to all of us. But short-term? Passwords have been, and remain, both an industry standard, and an industry frustration. Yes, they work, but there are significant issues that have put their existence in doubt. Nevertheless, for as long as they are still with us, we trust the information in this booklet will help you make stronger, more secure ones, and cause you less of a headache doing so. Finally, what we hope you have taken away from all this information is that, no matter where the future of digital authentication ends up, the ultimate responsibility will always rest with us, the user. In the 21st century it's up to all of us to be responsible with the keys to our most important online personal asset. Our identity.

Fidelity™ INTERNATIONAL



THE END.

© FIL Limited 2020.

Information contained in this booklet has been obtained by Fidelity International from public sources. Care has been taken by the staff of Fidelity International in compilation of the data contained herein and in verification of its accuracy when published, however the content of this booklet could become inaccurate due to factors outside the control of Fidelity International and this booklet should, therefore, be used as a guide only.

This booklet is published and distributed on the basis that Fidelity International is not responsible for the results of any actions taken on the basis of information contained in this booklet nor for any error in or omission from this booklet. Fidelity International expressly disclaims all and any liability and responsibility to any person in respect of claims, losses or damage, either direct or consequential, arising out of or in relation to the use and reliance upon any information contained in this booklet. Fidelity International means FIL Limited and/or its subsidiaries.

Fidelity™ INTERNATIONAL