The Indipendent

How safe is your password?

Qwerty. 1234. Ring a bell? We're forced to remember dozens of different codes – so how do you choose a rock-solid one? **Rhodri Marsden** explains

Passwords have never been that secure. Sentries of old might have considered the requirement for someone to whisper the word "Methuselah" to get past a checkpoint to be pretty damn stringent, but as soon as "Methuselah" was forgotten or passed on (deliberately or inadvertently), they may as well have abandoned the checkpoint and put up a sign saying: "Come on in."

Despite this, the almost laughably antiquated system of password protection has persisted in the internet age, securing our finances, our personal details, and those of slaughter-happy characters we've created in games such as World of Warcraft. These sequences of letters are usually recognisable words that are convenient, easy to remember and, we imagine, impossible to guess. After all, we came up with them unprompted, we didn't write them down, and didn't reveal them to anyone else.

But we're spectacularly unimaginative in our choice of passwords, and despite constant reminders that this represents a security risk, we blithely carry on using them, reassuring ourselves that we haven't been scammed thus far. But that's a bit like wandering blindfolded around busy town centres and saying: "Well, I haven't been hit by a car yet." But passwords will persist, not least because we're hugely resistant to anything more complex.

"They're the least worst in a series of bad options," as one security consultant recently pronounced. Remember our annoyance when British banks started issuing devices such as Barclays' PINsentry to implement a new level of security? We hated the inconvenience, despite them significantly reducing levels of bank-account fraud. We value convenience over security, right up until the point where that security is breached. So Arsenal fans persist in using "arsenal" as a password and deeply resent having to change it, despite the fact that it's one of the most easily guessable passwords they could possibly choose. (Liverpool supporters are just as bad, incidentally.)

Whenever the news features security breaches, from celebrity Twitter accounts to personal data leaks, weak passwords are often to blame. Our laziness in this regard is revealed in statistics that would be hilarious, if the implications weren't so serious. According to data gathered by Mark Burnett, author of the book Perfect Password, 98.8 per cent of us share the same 10,000 passwords. Many online security systems are built to withstand repeated incorrect guesses, but if they aren't, a computer could quickly zip through 10,000 attempts and gain access within a very short space of time.

Nearly one in six people will look at the list below of the top 10 passwords and passcodes and recognise theirs instantly; it seems incredible that "password" is still the most popular password – but it is, with 123456 trailing close behind. "5683" might seem at first glance to be a pretty random passcode or PIN – but it spells out "LOVE" on the keypad, and that's as much of a gift to hackers as

the ridiculously common password "iloveyou". These kind of careless, forehead-slapping mistakes are widespread within companies, too.

So why are our passwords still so predictable? According to Burnett, the common advice we're given – particularly to mix letters and numbers, as "pass123" evidently does – is misguided. "People just aren't as savvy as they think they are," he says. "For example, many people try to be clever with passwords like ncc1701 or thx1138, but these are the ship number for the starship Enterprise and George Lucas's first film respectively, and they're incredibly common. Rather than bothering with how many capitals, numbers, and symbols we have in our passwords, we should be concentrating on making them longer."

There are three ways a password can be compromised. The first is simply to ask us what it is. Social-engineering techniques can persuade us to give it up very easily – for example, via a rogue email purporting to be from a bank. The second is to have a guess, and as we've seen, 10,000 guesses will hit paydirt 98 per cent of the time. The last is brute-force cracking, where all the potential combinations are laboriously worked through until the right one is chanced upon – and that's where the length of password becomes crucial. Pop along to the website howsecureismypassword.net, tap in an eight-character password, and it'll tell you that a desktop PC can guess it in a matter of hours. But extend that to a 12-character password, and we're talking several centuries.

"If your password contains 15 characters or more, it no longer matters how random it is," says Burnett. "It doesn't matter if there is an English word in there somewhere, it doesn't matter how many numbers or symbols you use, it doesn't matter if you use the same letter too much, and it doesn't need to be changed every 30 days." Many techniques for password selection involve mnemonic methods – indeed, that's what I've always tended to do; for example the initial letters of a phrase, i.e. "You were only supposed to blow the bloody doors off" will generate "ywostbtbdo".

The other issue that consternates the password-choosing public is the knowledge that the same password shouldn't be used across every website we log into. But the mental energy it takes to retain more than two or three passwords encourages us, once again, to be lazy. Services like 1Password, KeePass and LastPass offer a convenient "remembering" facility, where all you have to do is provide a master password and it does the rest of the work for you. And while LastPass was subject to a hacking attack back in May, Burnett still recommends using such services - with the proviso that the master password is strong, and long. "The LastPass issue shouldn't have affected anyone with a strong enough master password," he says. "Mine is 24 characters long – but there are services like KeePass which keep all the passwords stored on your computer rather than online, so you don't ever lose control of the data."

Will passwords ever become obsolete? You'd hope that an alternative would soon emerge to save us from our own uselessness. Security expert Markus Jakobsson has been working on a system he calls "Fastwords", where passwords are replaced with a combination of three words that you can type in, in any order, to gain access. If you forget your fastwords, prompting you with one of them helps you to remember the other two.

Meanwhile, researchers at the American University of Beirut are engaged in a project called "Optimising Password Security Through Key-Pattern Analysis". This measures the typical time it takes for you to type in your password, calculating the pauses between the keystrokes; it can thus distinguish between the way you enter it, a stranger enters it and a computer enters it. If it senses you're doing the typing, it lets you in.

It's these systems that may provide the solution to computer security, rather than fobs, smartcards or fingerprint readers. "Passwords will never be obsolete," says Burnett. "A smartcard by itself is strong, and a password by itself can be strong, but used together they are much, much stronger." As long as that password you've chosen isn't "password", of course. Consider this to be your umpteenth warning, of what will probably be umpteen more.

Do you use one of the most common codes?

These are currently in the top five passwords in use online. If you use one of these for anything - email, banking, social media - you may as well not have a password at all.

1. password

2. 123456

3. 12345678

4. 1234

5. pussy

And these are the top five iPhone passcodes, representing some 15 per cent of all iPhone passcodes in use today. There's good reason to suppose that this applies to cashcard PIN numbers that people have chosen too; something that isn't based upon a memorable pattern on the keypad might be a better idea.

1. 1234

2. 0000

3. 2580

4. 1111

5. 5555