Top secret; for your eyes only

Michael Norell

Consultant Interventional Cardiologist and PCI Programme Director, The Heart and Lung Centre, Wolverhampton, WV10 0QP

(Michael.norell@rwh-tr.nhs.uk)

We continue our series in which Consultant Interventionist Dr Michael Norell takes a sideways look at life in the cath lab…and beyond. In this column, he considers the pitfalls of passwords.

Has it only been for the last 20 years or so that our professional, domestic and financial integrity has required us to protect ourselves with a personal identity number (PIN) or password of some description?

Memorising such a catchy or familiar word, an easy sequence of figures or a combination of both, has now become, not only commonplace, but an evolutionary necessity. I presume that it was the electronic revolution that 'sparked' the need for this type of validation. Previously, a hastily scribbled signature, which – to the untrained eye – appeared reasonably similar to the scrawl on the back of your credit card, might have sufficed.

Any form of registration, transaction or authorisation is accompanied by your need to transmit, insert or 'punch in' an indication that the process in question is not only *bona fide* but also being vouched for personally with a sign that *only you* would know. Right now there must be a wealth of electronic interactions available to us, such as when we boot up our laptop, 'log on' and register with a website or top up with cash at a hole in the wall.

Surely, all of us must be currently using a dozen or more passcodes of some sort. Add to this the encryption that is now quite rightly part of the transfer of any National Health Service (NHS) information, and the list of events demanding our authentication starts to become unwieldy.

The burden

The question is, do you try and use the same word or number sequence for all your requirements, or do you memorise a constantly expanding variety? I confess that I find these demands on my ever-dwindling mental faculties, an increasing burden. For that reason, I have tried to use the same password for all eventualities. This slightly risky strategy has worked thus far, although admittedly I haven't checked my bank account today.

Your 'mother's maiden name' appears to be a common word suggested by banks and other institutions in the hope that it will assist the user in verifying a transaction. However, in the era of the extended family it may not be apparent to some individuals as to what this actually was.

This 'one-word' approach, while convenient, has been made more difficult because some systems require a password to be changed on a regular basis, e.g. monthly. Adding a digit to the end of your keyword that you simply increase by one every 30 days or so, is an option as long as you can remember what the last one was. I suppose you could always use the name of the month as a password but that strikes me as a bit of a giveaway, and anyway what do you do in 12 months' time?

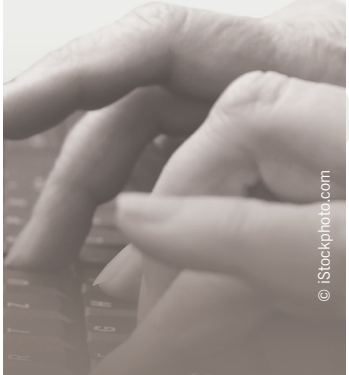
As for numeric codes, I currently need to remember at least five (or is it six?) number sequences, in order to use various credit or debit cards, set – or more usually, silence – the house alarm, open our wall safe and unlock my bicycle. I have run out of birthdays or the novel use of other memorable dates that could be entered in reverse order or with each composite figure increased by one. Of course the danger is that if you make the solution too obtuse, you won't be able to work it out yourself.

The pressure

Whether a word or a number sequence, the pressure is on you when you are instructed after your first failed attempt that you have only two further tries to get the thing right. Otherwise your plastic card is swallowed, your computer will not allow any kind of access for at least five years, and a large hand will spring out from the screen and slap you on the side of the head.

It does not help when the letters or numbers that you have, thus far, painstakingly entered, appear as a lengthening line of large black dots, and, therefore, do not indicate whether or not you have already made that fatal error. Incidentally, I have actually tried typing a line of seven black dots in the 'enter your password' field; it doesn't work. Furthermore, I am sure that as a result of this quite reasonable wish to further my e-knowledge, the computer thought to itself that the operator was clearly an idiot (probably spot on there) and shut down in disgust.

I anticipate that Darwinian principles will mean that Homo sapiens with less capacity to rapidly, and reliably, recall keywords or numbered sequences, will be disadvantaged. Natural selection will mean



The complete collection of these and other articles is now available in a book 'The Oblique View'. Further details can be obtained from Nikki@tfmpublishing.com or www.amazon.co.uk

that there will be preferential survival of the e-fittest, not so much because of the opposable thumb, but more as a result of our ability to manipulate other digits.

The danger

But what is the real danger? What is the genuine concern? It is not about being thought of as having purchased some dodgy DVDs online (allegedly), having your bank account drained or even your bike nicked. It is the ultimate crime of the electronic era, namely the theft of your very *identity.*

This modern day contravention of natural law is far removed from the simple acquisition of a false passport. The means to possess such a hallowed document was laid out in easy-to-follow steps by Frederick Forsyth in his classic 1971 bestseller "*The Day of the Jackal*". Since then the loophole in birth and death certification that allowed this chicanery, has been closed (I hope), but the twenty-first century version of this demeanour goes far deeper.

How can we *prove* who we are? Holding up a mirror and exclaiming: "Yes; that's me!", hardly stands up in court and opening a wallet and spreading out a collection of plastic cards, all with the same embossed name, won't cut it either. A driving licence or other photographic evidence that puts a name with a face could help, but may already have been falsified. Even colleagues, friends and family, all of whom would swear that "you are who you say you are", may have been taken in by a long-standing plan cooked up to replace one individual with another.

It is a frightening prospect to imagine that somewhere out there could be another Mike Norell (spelt correctly, *I would insist*) using my bank account, my password, my computer log-ins and – come to think of it – having unauthorised access to my bicycle. (Believe me; it scares me as much as it does you.) But, I guess as long as he also pays my bills, I shouldn't complain. He (for I presume this doppelgänger would have to be male) might actually be a wealthy and extraordinarily successful – if a tad unscrupulous financier, in which case it might then be worth me stealing (back) *his* identity. That should be fairly easy … shouldn't it?

Finally, in the spirit of dogged enquiry and openness for which this publication is renowned, I now intend to break new ground in journalistic investigation. I am herewith going to publish my universal password, used for all my financial and professional transactions. I will then scour the ether to see whether there are any signs of me emerging in an alternative guise, turning up in questionable circumstances or in other ways being surreptitiously cloned. Here we go; be sure to make a note of it: *******