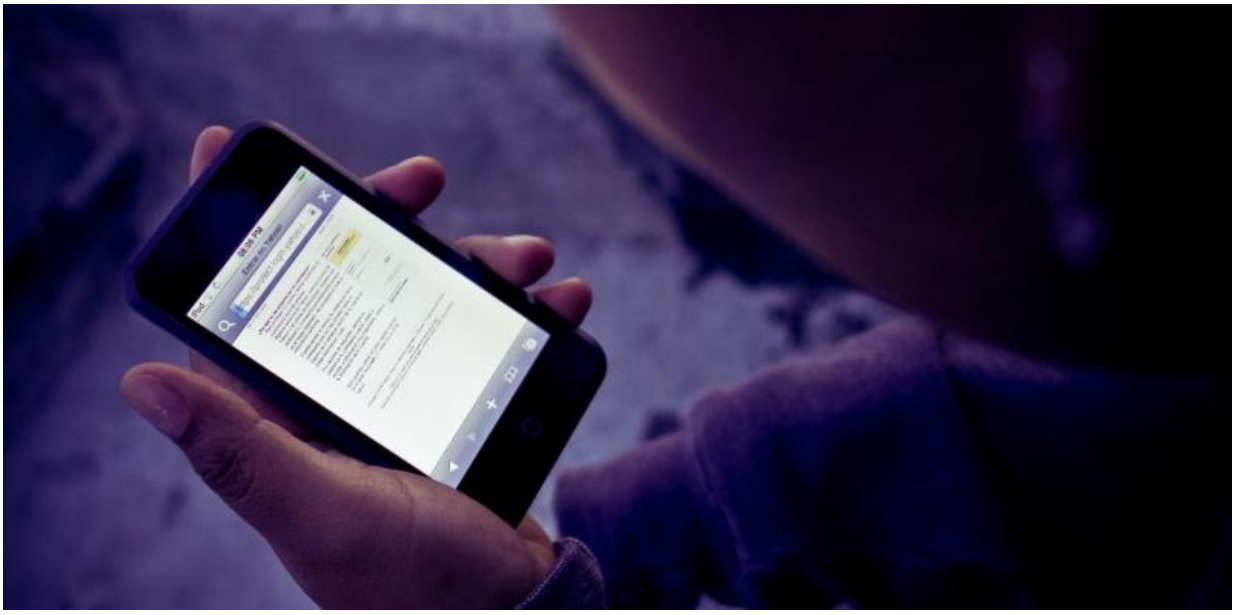
Security vs. usability—that's the choice we make with passwords

September 3 2015, by Mike Johnstone



How secure are your passwords? Credit: Flickr/Krynowek Eine , CC BY-NC-ND

We all need some kind of authentication process if we are to access information systems at work or at home. We know why we need to do it: to make sure we have access to our data and unauthorised people don't.

So why do we routinely ignore such advice, particularly given the constant advice from cyber security professionals about the need for

strong passwords that are changed frequently? It seems there is a significant disparity about what we do and what we want: is it security or is it usability?

Most authentication we encounter today is typically implemented in one (or more) of three ways:

- Something you know (such as the humble password)
- Something you have (a smart card)
- Something you are (a fingerprint).

Many systems use a username/password pair for access control, largely because the interfaces to most systems have typically been some sort of keyboard. Some smart phones use a PIN or fingerprint and bank ATMs use a combination of something you have (a card) and something you know (a PIN).

The trouble with passwords

Having a long random password is good advice. It provides a measure of security for guarding access to important information, such as your online banking account.

Unfortunately, when faced with having to remember several random fifteen character passwords (characters being A to Z, a to z, 0 to 9 and an assortment of other printable characters such as ! @ # $ and %), most users apply a judgement to the value of the information protected by the password and act accordingly.

Some accounts may have a relatively weak password, because of the cost of undue information leakage or harm to the owner if the account is compromised. Other accounts might have a stronger password, because users don't want their money siphoned off by a cyber-criminal. These are

judgements about the perceived value of the information.

How safe is your password?

If you must use a password, what makes a good one? How fast can a password be cracked?

There are several web sites that publish lists of common passwords. I have used a list of 14 million passwords as a test with a local science discovery centre in Perth.

Attendees at the centre (mostly high school students) were asked to enter what they thought was a secure password and this was checked against the list. If not found on the list (a rare occurence), the password was sent to a fast computer for further processing.

This computer could crack a random six character password in under two seconds, using a brute-force attack by trying to match "aaaaaa", then "aaaaab", then "aaaaac" and so on through all combination of six characters.

It was surprising how little the fast computer had to do. Many users assume that words or phrases taken from well-established literature are somehow secure. They are not (forget anything from Lord of the Rings or War and Peace).

A longer password takes longer to crack. A random 15-character password might take a week, but then the argument comes back to the time value of information. If a cyber-criminal has to wait a week, your account will still be there and will you change your random 15-character password every week?

One way to add an extra level of security to your password is to enable

any two-step authentication, whereby another code is sent to a device, such as your mobile phone, after a password is entered. Plenty of online services already offer this service.

We need some other authentication

If the humble password is not suitable due to usability issues, then there are alternatives such as the popular pay wave contactless payment system for bank cards and travel cards, with no password required for small transactions.

The risk is that if your wallet or purse is stolen, small amounts can be siphoned from your account before it is blocked. Nonetheless, tapping a card is proving to be popular with consumers and with retailers, so convenience wins over security.

Biometric methods, based on some physical property of the human body, are attractive because a person doesn't need to remember a password or carry a card. Smartphones and computer operating systems already use fingerprint scanners to provide a simple and effective means of authentication.

Other biometric devices in use include retinal scanners, iris scanners and voice recognition. Despite what is seen in popular movies, no-one likes having a laser shined into their eyes, so voice recognition might be the way forward.

But there are known issues with biometric technology. But those issues are the same for any authentication system. Current error rates for single-fingerprint devices are approximately 2% at best – not good enough to be used on their own yet.

Some systems don't rely on matching the actual fingerprint, but match

other behavioural properties of a user. For example, the angle and velocity of fingerprint scanning, which are properties that are different for each person, are measurable and repeatable. This defeats a physical attack such as removing a person's finger in an effort to impersonate someone.

Returning to the ATM example: for now, we are bound to cards and PINs due to their low maintenance and production costs. From a customer's point of view, it would be simpler to speak to an ATM and ask it for cash, once your voice print linked to your account has been confirmed. This is a much more user friendly (and safer) future.

Ultimately, until more robust security alternatives are widely accepted (and implementable at low cost), those who continue to ignore the advice on passwords much seriously ask what balance of security and usability they prefer, and what price they're prepared to pay for weak security?

Source: The Conversation