

Keep it Secret – Keep it Safe

By Bruce McGregor, Director



Or of 'PINS' and 'Passwords'. Having recently been in the unfortunate situation of having lost my wallet I have, as a consequence, had to go through the process of replacing all my Bank Cards. During this unavoidable 'refresh' process I was presented with both the requirement and the opportunity to change and update associated PIN numbers and passwords. It was at this point I had the not uncommon thought "Oh no, how am I going to come up with yet more passwords or PIN numbers to memorise?" Particularly ones which my ever forgetful brain can remember easily and which are not the same as ones I already know!

As we all use technology more and more and particularly through the Internet for: paying for things; joining clubs; access to social media sites etc, we are also increasingly bombarded with the requirement to come up with more and more of these unique but memorable PINS or passwords to ensure, not least, that our valuable personal information or identity is safe and secure. But as our brains 'tilt' under this overload of requests to submit yet another bit of important info to memory I couldn't help but think "Surely there is something out there to help?" lest I fall into the traps of 'bad password creation habits' which the industry already knows many people do. For example, like using existing numbers such as their telephone numbers, house numbers or date of birth, for PIN number creation. While these numbers are easy to remember they are, nevertheless, easy to break too.

We need to ensure that our passwords are 'strong' so we don't make it easy for hackers to guess them. I found it shocking to discover that the most commonly used password is 'password', clearly not much of a challenge to an intelligent hacker! Plain words are not advised as they are also too easy to hack. A strong password should be, not least, a combination of letters, numbers and keyboard symbols; a mix of upper and lowercase and at least seven characters long. PINS should be unique, don't use the same one for more than one card, don't write it down, don't store it in your phone and... "Oh no, my brain's beginning to hurt again!"

What can we do to help us in this situation? One approach to this 'memory challenge' is to accept the inevitable, as more and more of these passwords and pins need to be remembered

and more 'cryptic', and to seek assistance from software technology to help our poor beleaguered brains!

Possible solutions come in a number of guises, with 'Password eWallets' being one. These secure highly encrypted software solutions, installed on a PC or your mobile device, allow for the safe storage of not just passwords but also card details, PINS and much more.

These are, in fact, accessed by their own secure PIN or passwords but they should mean that we need to remember far less of the ones stored inside. Another advantage is that we can make our passwords 'stronger' as we don't have to worry about memorising them. However, while I think these may well be a good idea for a PC used in the security of one's own home, to safely store our logins and access to our numerous shopping and secure Internet sites, I'm not so sure that using such a solution whilst out 'in the wilds' of a public street, for example, would be such a good idea! Also, which one do you choose or more importantly can you 'trust' with such important personal information?

We all know why we need to keep such important information highly secure. We are often told that bank card and identity fraud is on the increase and that we need to be ever more vigilant. Recent statistics back this up, with research by Card Watch, a UK banking industry initiative that aims to raise awareness of card fraud prevention, showing that card fraud losses have risen, in the UK alone, from a not insignificant £135M back in 1998 to in 2008 a staggering £609M!

"But I thought Chip and Pin was supposed to significantly reduce card fraud issues", I hear you ask. Well, in fact it has! In many standard or 'high street' transaction processes, APACS (the UK trade association for payments) identified the success of Chip & PIN with statistics revealing that between 2004 to 2007 losses on transactions on the UK high street reduced by 67%.

Overall, however, there is still a significant increase in card fraud year on year. In more recent years, it appears this is almost certainly due in large part to a rise in card-not-present (CNP) fraud, almost certainly fuelled by the huge increases in both the number of people shopping online and over the phone, and the number of retailers offering telephone or online shopping services. In fact these CNP fraud figures are growing every year and now make up more than 50% of all credit card fraud.

So what is the industry doing about this increased CNP card fraud? Current online software solutions are available to bolster security further. Verified by Visa and MasterCard's SecureCode are secure payment systems that aim to prevent criminals from using stolen card details for Internet transactions. These are password-protected services that enable financial institutions to confirm your identity for the merchant when you are using a card to pay online. Enabling merchants to confirm your identity in this way puts another barrier between criminals and your information, but while they do increase security unfortunately they also require us to remember yet more important passwords.

Also, with further hardware enhancements, chip and PIN cards may further help prevent Card Not Present (CNP) fraud. To this end Visa is testing out a new card, with a computer screen and keypad embedded into it, in the latest move to counter the Internet fraud and in particular this

Card Not Present (CNP) issue. The technology in the card gives users another extra level of security when they are shopping over the phone or internet.

These new 'Emue' cards are designed to put an end to this so-called "card not present (CNP)" fraud. When on a retailer's website, you will be asked to type in the credit card number and three-digit security code as normal. The website will then ask purchasers to type in their Emue code. To get this code, consumers will turn over their card and use the keypad on the back of the card to type in their Personal Identity Number (PIN), as they would in a shop. An 'on the spot' randomly generated unique four-digit number will then pop up on the card's mini screen. The shopper types that four-digit number into the website. This extra code – which changes every time the owner of the card uses it – will be verified by the credit card company's servers and allow the transaction to go through.

This latest battery-operated card, fractionally thicker than a standard credit card, should be in consumers' hands soon if trials are successful. Visa estimates the cards will be distributed to customers from next year. The battery life should last at least three years, ensuring it runs out after the card has expired.

In trying to answer my question with respect to how could I be helped when it comes to PINS and Passwords and the inevitable concerns with respect to potential fraud, I discovered that I raised as many questions as I found answers! While the industry appears to be doing much to prevent fraud it also comes down to us as individuals to be as vigilant as we can be. There are in fact ways we can get help and I shall certainly be looking into these in more detail. Now, where's that brain trainer gone?