

Online Security – A Different Perspective

1 Sep 06

By Sherman Tan

Over the past few months, there have been numerous press reports on the emergence of fraudulent websites that almost resemble the real ones, increase in phishing incidents and security flaws in bank's internet banking websites.

In several countries, the banking industries have started various initiatives to educate consumers about phishing, scams, spam mails and offer tips on safe online banking and e-payment. One such site is the BankSafeOnline which is an initiative by the UK banking industry. The website is at http://www.banksafeonline.org.uk/phishing_examples.html.

The Monetary Authority of Singapore (MAS) has instructed banks offering online banking services in Singapore to enhance their online security by the end of the year.

Since 1996 when the first internet banking website was launched, most banks' online banking service is accessible using a static user ID and assigned password. While the user ID and password can be changed by the user, this authentication process rely fundamentally on what the user knows; ie his ID and password.

Second or two factor authentication (usually also refers to as 2FA), however requires the user to possess something else in addition to what he knows and that something must be uniquely associated with the user.

2FA is not a new technology and has existed in several forms for many years. The most commonly used is the ATM card and the PIN.

In the early days of Online PC banking, many Nordic banks provide its customers each a personalised sheet of paper containing some 20 to 50 set of 3-4 digit numbers. After entering the usual static User ID and PIN, the customer enters one set of these numbers for additional authentication. After successful login, the customer struck off this set of numbers from the sheet and the process continues for each subsequent login until all the number sets are used up. A new sheet is then requested from the bank.

This is the simplest form of 2FA and yet it serves its purpose well. Firstly, even if the user ID and password have been compromised through "shoulder surfing" or captured through key logger program, the hacker does not possess the personalised sheet of paper and is unable to supply this unique information assigned to the legitimate customer.

While it is simple and cost effective, the solution has its drawback. Firstly the paper is either easily misplaced or damaged; the algorithm used for such implementation is considered weak in today's security technology and thirdly, it doesn't appear sophisticated in today's world – archaic to many.

Several 2FA devices and technology emerged over the past 10 -15 years and the most commonly used device is the security token that generate a random one-time password every minute or so. Some more secured implementation requires the owner of the token to enter a PIN in the token before a random set of password is generated.

These security tokens which are costly are initially used by banks for high-value financial transactions and inter-party payment. Gradually, these tokens are used for authenticating user access into secured private network and subsequently extended to business customers who are using corporate online banking services.

To banks, security tokens seem a natural choice if 2FA is made a mandatory requirement for the general consumer banking customers especially for banks who have already set up the infrastructure to support tokens for their corporate banking customers. Moreover, procuring tokens in large quantity will reduce the unit cost per token. And what are the concerns?

In mid July this year, it was reported that a group has set up a “man-in-the-middle” attack to compromise? the use of security token. The link is at http://blog.eweek.com/blogs/larry_seltzer/archive/2006/07/11/11339.aspx

From the operational and maintenance perspective, the general consumer banking customer base for large banks using online banking could be in excess of millions and educating this huge base of customers is a challenge. Moreover, there are maintenance and support issues such as misplaced tokens, damaged tokens or simply when the customer is overseas and is unable to login because he left his token back home. Then there are customers like this writer who has online banking service with 5 different banks – imagine the hassle of keeping the 5 different tokens.

On the bright side, the implementation of security tokens could potentially lead to the higher usage or subscription of online banking service as some customers in the past have avoided using online banking due to security concern. Peak hours could also spread out as customers who use online banking in the office may now switch to banking from home as they are unlikely to carry their security tokens all the time. Banks could also offer more products, higher value transactions and account opening over the internet as security token reduces the risk of impersonation.

However, is security token the silver bullet to online security issues?

Before we answer this question, let’s look at the physical world. We will use the motor highway as an analogy; though not a perfect model but a useful one to illustrate the key points.

Over the years, roads and highway are built by public and private organisations to facilitate point-to-point travel and when the fuel locomotives become common sight on these roads, accidents occurred. To curb accidents, traffic rules and laws are set up. Over the years as car manufacturers develop higher speed vehicles, they also take responsibilities to test these vehicles for safety, ease of use and efficiency. Drivers are required to pass tests before they can drive on public roads. It is also laws in many countries requiring the vehicle to be insured when cruising on public roads.

Why can’t the internet and online banking adopt some of these features?

Firstly, banks that offer online banking service (similar to car manufacturers) must ensure that their services are well designed, tested and secured. Internet service providers, regulators and infrastructure builders must collaborate to educate the users of the internet and provide ancillary services to improve the usage and experience. Users of internet services should acquaint themselves of “highway codes” of the internet; knowing when to turn, when to stop and when not to drive over the cliff.

Banks, regulators, internet service providers and users know that there are risks associated with the use of online services but the benefits outweigh these risks. One of the mitigating actions is to introduce insurance to cover online banking services. In may not be too distant in the future when user of internet who passed an “internet highway code” test is given a lower insurance premium compared to those who didn’t.

When the various parties understand their roles and contribution, the internet highway will be much a much safer place to cruise for performing online banking services conveniently and safely.

The writer is the Principal Consultant & Director at Innovar Pte Ltd (www.innovar.com.sg).