

# Protecting Online Transactions

**Transactions performed online are exposed to a myriad of evolving security and fraud based attacks. Businesses and consumers must be aware and vigilant as online activity is no longer constrained to a PC as the global proliferation of mobile devices grows. This paper discusses this new dawn for online fraud and the need for answers.**

With emerging terms like crimeware, malware, rootkits, trojans, phishing, spear phishing, pharming, man-in-the-middle (MIM) and spyware, it may be incredible to think that the level of online transactions continue to grow rapidly. Yet to what extent does the consuming public recognise these threats and moreover the businesses & governments providing the online services in the first place?

## **Is your identity at risk?**

This paper focuses on online transactions in recognition that attacks are not aligned to payments activity alone. Gathering and taking over your identity, including user names, passwords, biographical data and secret questions/answers are all targets for a 'cyber'-criminal.

A recent Harvard & Berkley report notes three areas of reliance for phishing attacks: lack of knowledge, visual deception and lack of attention. The UK Government is looking for its Citizens to be more aware with the launch of a 'Get Safe Online' website; while Australia has '[www.protectfinancialid.org.au](http://www.protectfinancialid.org.au)'.

Awareness about the dangers in exposing your personal information on the web is wanting. Research by Sophos, a US IT security firm shows that 40% of Facebook users are too free with their personal information including addresses, date of birth, phone number and email addresses.

A report issued by Symantec in March 2007 notes that stolen credit card details are selling for US\$1 to US\$6, and biographical & identity data is selling at US\$14 to US\$18.

Hacking of websites has moved from showing off and making sure people knew who you were to a sophisticated and now increasingly hidden activity. Many consumers consider the security of their PC with tools and firewalls, yet how many subscribe to the updates or renew?

Importantly, what security do consumers consider when using their web-enabled mobile phones to logon to their bank, favourite website or to download email?

## **The latest threats**

The sophistication of web based attacks can not be ignored, and unfortunately many attacks are much harder to detect or trace. One group known as the 'Rock Phish Gang' is such an adversary. Comparing the longevity of an attack; 'normal' phishing attack sites stay up on average 58 hours, yet Rock Phish attacks are lasting over 94 hours before being shut down.

Phishing attacks remain highly focussed on financial institution brands accounting for more than 96% of reported incidents. Australia & New Zealand brands account for 2% of attacks according to RSA's July 2007 report. Yet unexpected brands and sites are threatened.

Recently, it was reported that the Sydney Opera House home page had been compromised. A new wave of 'drive-by-attacks' sees trusted websites broken to install a javascript that hosts malicious code. When people access a site, the code infects their PC or device. This type of attack use Rootkits that hides the malicious code from other programs and operating systems including anti-virus ware.

RSA further highlights kits are being offered on the web for free supporting the developer in their quest for greater reach of fraudulent earnings through man-in-the-middle attacks. How can you combat such a diverse array of cyber-crime? Is it possible to be ahead of them?

### **Approaches to protection**

Providing strong security for online services is often costly and can reduce usability for the end-user. The balance of cost versus usability is difficult for many businesses as they seek greater adoption of e- and m-commerce, while providing more convenience to their customer base, yet protecting their own brand by remaining trusted.

Protecting online transactions is not only the domain of the business or government offering the service but also the consumer. It is essential that web based devices are loaded with current anti-virus & spyware protection tools. Importantly, your own vigilance is essential as you traverse across the internet. When it comes to transacting however, how are you protected?

Business and Government have numerous tools available to secure their sites and your interaction with them; some are overt, others remain covert!

Many use IP address tools to confirm that a person logging in is using a regularly used PC and internet connection or Transaction Anomaly Detection to track variances and mitigate fraud exposure. Techniques including secret questions only the valid user should know the answer of or the use of secret images that again the valid user should recognise are scenarios that allow both the business and consumer to confirm that the other is a valid user or website.

Many widely used solutions do not protect you against man-in-the-middle attacks or other emerging

techniques. There is increasingly a reliance on multiple solutions and channels to provide full security of your identity and your finances.

### **Are you protected?**

Some banks have issued a token that provides a One Time Password (OTP) for each unique logon. The dependency is the consumer must carry an additional device and have it with them each time they wish to transact. This is a high cost solution, which in itself is open to compromise especially by friends and family use.

The use of mobile phone SMS based solutions does reuse an existing consumer device; however SMS is not reliable if you require a real time delivery of an OTP. Equally, interactive use of SMS to transmit PINs or passwords to your provider will leave a trace in your sent items folder unless cleared.

Yet while you may see the secret image on your website, or answer the secret question correctly, the data may still be received by a cyber-criminal undertaking man-in-the-middle fraud. So what now?

### **Being detection minded**

Securing online activity requires a complete yet interactive separation of your login or confirmation credentials from the channel in use. Ie Transact on-the-net, authenticate off-the-net.

To be effective, the consumer must be able to readily use and rely on the solution. Having interactive use allows the user to be authenticated, the transaction to be confirmed or declined due to either incorrect information (MIM attack) or the transaction was not initiated by user (ID theft).

With providers of detection tools and security solutions working collaboratively, the ability to detect and record fraudulent payments and identity theft, work towards closing the up-time of crime based sites.