

September2007



WHITEPAPER

MANAGING YOUR IDENTITY IN THE ONLINE WORLD



TRUSTDEFENDER

www.trustdefender.com

TrustDefender
(Symbiotic Technologies Pty Ltd)
Phone: +61 2 9566 2677;

5 Gladstone Street; Lilyfield NSW 2040
Australia
Fax: +61 2 9566 2688;

Website: www.trustdefender.com
Email: info@trustdefender.com

Managing your identity in the online world | Peter Ager

Managing your identity in the online world

Contents

Foreword	3
Three types of person or entity	4
The Key Questions for the consumer or end user	5
The Key Questions for the service provider	5
Customer Resource Management (CRM) and “Know Your Customer” (KYC)	6
Customer Identity Risk	7
Identity Theft – what is it?	8
Identity Fraud	9
Who is affected by Identity Theft / Identity Fraud	10
Identity Theft – and the internet	10
The future	12
Identity Management – an imperative	12
Managing your identity in an online world	14
How we prevent the loss of your identity in a material world	14
Managing online security – there is no compromise	15
Identity Theft, Brand Protection and Customer Loyalty	16
About the Author	17
About TrustDefender	17

© Copyright 2007, Symbiotic Technologies Pty Ltd. All rights reserved. No part of this publication may be reproduced or stored in a retrieval system or transmitted in any form or by any means, without the prior written permission of the copyright holder. Symbiotic Technologies Pty Ltd is the sole copyright owner of this publication.

Managing your identity in the online world

Foreword

Ecommerce, or Electronic Commerce, is one of the most important aspects of the internet to emerge in the past 20 years, originally developed to enable the online processing of financial transactions between the major financial services institutions and their larger corporate clients.

As the enabling technology and the range of services have developed through the course of the past 20 years, consumers and businesses alike have adapted to the growth in internet based commerce to the extent that we now accept the use of the internet for:

- Exchanging information – including personal or confidential business information,
- Buying and selling of goods and services and
- Making payments or accepting payments.

With this growth in online activity and the ever increasing proliferation of services that leverage the internet, consumers and businesses alike are using the internet to provide ever increasing amounts of personal and confidential details to third parties including their banks, online services and even the government. In addition we are seeing the emergence of Second Life and social networking websites that are used to share the most intimate and personal aspects of our lives not just in the home but also in the corporate environment.

Modern electronic commerce typically uses the World Wide Web at least at some point in the transaction's lifecycle, although it may encompass a wide range of technologies across multiple touch points including email.

With this progress, there comes an increased level of risk associated with the exchange of and use of personal and business information across the web.

The recent arrival of online social networking websites such as Bebo, YouTube, MySpace and Facebook has created a new avenue for sharing personal details on the internet and with that comes the added risks. With more and more intimate personal and business related details now being exposed to the greater World Wide Web, then as a result we see an increase in the level of online fraud and identity theft!

In effect, the internet not only enables people to exchange information and to buy or sell goods and services immediately, it also reduces or eliminates the traditional barriers of time or distance. Business can now be conducted at any time of the day or night and from any location around the world.

The internet also exposes the consumer, business, financial services providers and other users of the online services to a greater risk of exposing personal and confidential information. In other words, there is a greater risk that confidential personal and business details can be used to create false identities that can then be used for fraudulent activities including money laundering, terrorist financing or other criminal related activities including defrauding the true owner of the person or business identity.

Managing your identity in the online world

The following paper discusses these issues in further detail and in turn provides a number of recommendations on how to best ensure that when exchanging personal and confidential information via the internet, the end user can do so with a level of confidence that their information is safe and secure and cannot be accessed by third parties who will only use this information for their own advantage – fraud being their number one objective!

Three types of person or entity

In dealing with online commerce and the exchange of confidential personal and business related information, it is necessary for the user to understand that when dealing with a third party, one also needs to understand that the person or business they are dealing with may either be:

- **Good** – the people and businesses we know and trust (the white list)
- **Bad** – the people and businesses we must avoid (the black list) or
- **Suspicious** – people and businesses we have little or no knowledge of in terms of past dealings but may become a regular client / customer (the grey list)

However, when dealing with an online business or person, it is often difficult to determine that the web site we are using is safe to use as much of the spyware problems that we encounter, in our day to day online activities, are usually the result of either receiving email or from visiting web sites that turn out to be untrustworthy or simply malevolent.

In fact, most of these encounters arise when we either knowingly or unwittingly visit a site for the first time or when we accept offers under the guise of advertising software or some overly worded end-user license agreement (or EULA's) that are many pages in length. However, when we do finally run the offending software download, the resulting software ultimately ends up on the end user's computer simply because they browsed a site that simply does not pan out!

The dilemma we face is that we cannot determine if the site is good, bad or otherwise suspicious! Online security solutions and virus scanning solutions can only offer a limited level of protection in that they provide a service that either lists:

- **“Bad sites”** through the use of “black lists”
- **“Good”** sites through the use of “white lists” and / or
- **“Suspicious Web Sites”** and other malware – otherwise known as “grey lists” – to indicate that such sites and software should be used with caution until their bona fides are known!

Managing your identity in the online world

The Key Questions for the consumer or end user

During the start and throughout each and every online session, the consumer or end user needs to keep in mind that the privacy and confidentiality of the information that they exchange with the service provider may be at risk. To guard against the risk of exposing personal and confidential details when using an online service, one must first have an understanding of:

1. **Who** am I dealing with – who is the service and is it the genuine article?
2. **What** are they going to do with my details? and
3. **Why** are they doing it?
4. **Where** are they doing it? Will this information be retained and if so, will it remain confidential and thus remain in safe hands?
5. **How** are they doing it – is the information likely to be used to gain access to other personal / confidential details?
6. **When** are they doing it and how frequently are they likely to use this information?

Usually, the initial contact with a service provider such as a bank or merchant is through the end user accessing the service provider's internet site where the end user provides personal / confidential details that should only be known to themselves and their bank or service provider.

But, when we access online services such as web sites, the end user also needs to be vigilant as to whether or not they have accessed the genuine article and not a "phishing" site set up to shadow the genuine site with the sole intention of accessing your personal and confidential details.

Quite often, a "phishing" site may be just a window that opens to the genuine site but manages and maintains the traffic between the end user and the genuine site. So any exchange of details between the end user and the genuine host can actually be recorded and used by the "phishing site" to defraud the end user and the service provider as their activities emulate that of the end user – they have your personal details including login ID's, passwords and other pertinent security or personal details that may be required to authorise access to your personal and / or business records.

As online fraud increases, there is an ever increasing demand on end users to ensure they are using safe and secure online services to guard against the possibility that their personal details are stolen. This also includes ensuring that their current computer device is clean from malware, secure before and during any online transaction and that their intrusion protection is always up to date.

The Key Questions for the service provider

The same key questions addressed in the previous point also need to be addressed by the financial services provider or other online service provider both at the start of an online session and then throughout each and every online session with the end user.

Managing your identity in the online world

From the service provider's perspective, the service provider is obliged, in the end users eyes, to ensure that the privacy and confidentiality of the information provided by or to the end user is not at risk. To guard against the risk of exposing the end user's personal and confidential details the service provider such as a bank must remain vigilant when dealing with their online users and to ensure that they know and understand:

1. **Who** is the customer – i.e. who is using our services and conducting business with us?
2. **What** is the customer doing (or going to do)?
3. **Why** is the customer or user doing it – in other words, is this activity normal or out of character and thus potentially of a suspicious nature
4. **Where** is the user doing it – Home / Cafe / Office / Overseas – and is it possible to determine the health and overall security of their pc or the service they are using
5. **How** are they doing it – is this an online activity from a known user site or a foreign site?
6. **When** are they doing it – frequency as any out of character activity should be predicted from the known history or the metrics used to access the risks of each online activity

This sounds very much like Customer Relationship Management (CRM) as businesses need to understand their customers' online service activities, to manage their relationships with customers, including the capture, storage, analysis and protection of customer, vendor, partner, and internal process information.

Customer Relationship Management (CRM) and “Know Your Customer” (KYC)

The key to successfully managing the relationship with each and every online user by online businesses is to ensure that the online services are capable of not only handling the volumes of online transaction traffic but the business is able to leverage its customer data bases and the risk management solutions to ensure the most efficient customer relationship and experience.

Access to CRM based solutions also provides the ability to counter the increased demand for quality customer data including, online fraud, anti-money laundering and terrorist financing data. For example, financial institutions need to cater for the “... real-time, enterprise-wide dissemination of new information, that is distributed in such a way that it allows businesses to react quickly to it”. In the online world, this information needs to be available when the client is online – both to score the online session and to ensure the client receives a positive experience but also to ensure the activities fall within the norm for the level of and type of activity that they conduct online.

A common goal of both CRM and KYC is to “...drive the competitive business advantage to its ultimate limit whilst limiting or preventing online criminal activities including terrorist and anti-money laundering related activities”. In other words, the goal is to enable the “...instantaneous awareness and the appropriate response to events, as they occur, across the entire enterprise”.

Managing your identity in the online world

Customer Identity Risk

Online commerce and services pose a significant issue for businesses relating to “customer not present” activity where information is being provided by or exchanged with the online user.

The key issue for the online service provider is to know whether or not the end user is the authorised or genuine customer and not another party who has assumed the identity of a known customer or another party with the sole objective of using the identity to hide their true intentions or worse still, to use the identity for fraudulent purposes.

As we all know, we are constantly required to provide identification as evidence to open bank accounts, obtain credit cards, finance, loans and mortgages, to obtain goods and services, or to claim benefits from the government. But this also requires the physical presence of the customer at the point and time the transaction is being completed.

A customer’s identity is a valuable commodity – both to the customer and to the businesses with whom they conduct their online business. Both personal and business customers need a safe and secure identity to function in everyday life.

In the online world, the ability to secure and to verify the customer’s identity is limited as information provided by the customer, during the online session, needs to be verified, validated and possibly scored using risk rating engines that provide a higher degree of satisfaction that either the:

- Information provided by the new client is true and accurate or
- The customer is transacting from a computer, PC or mobile computing device that can be verified as secure and/or is known;
- Online activities of a current customer have been assessed against their CRM based risk profile and are scored accordingly.

In addition to the faceless nature of online commerce and activity, it is also borderless, which brings a new dimension to managing the identity of the online customer. That is, is the customer who they say they are or has the identity being offered by the online user been stolen or created to disguise the real modus operandi of the online user?

Any activity that suggests that the identity being offered does not score highly or cannot be validated should require further checks and verification of the clients details – with the provision of identity documents.

To address the possibility of potential fraudulent activity, the online business is in the best position to provide an end-to-end service that guarantees the safety and the security of the information and the transactions that are exchanged between the end user customer and the service provider during each and every online session.

The use of end point security solutions that integrate with the online service provider offers the service provider and the end user, the customer, the ability to control the online transaction and

Managing your identity in the online world

to prevent access to suspicious sites whilst ensure the end-to-end security of each and every online session. This also guarantees the end user, the customer and the service provider is operating in a safe and secure – point to point – environment that is in effect a one to one relationship.

After all, customer identity theft and the risk of identity theft affects all levels of government, business, commerce and personal activity and the criminals and even the terrorists who exploit the use of fraudulently obtained or created identities are smart – they can find the weakest links and exploit these to their own benefit.

With the increased surveillance measures now being applied by the security agencies including the anti-money laundering authorities around the world, the objective for online businesses, especially the financial services industry, is to prevent the use of false identities to:

- **Launder money** – sending “dirty money” through the wash
- **Facilitate terrorist activities** – using clean and “dirty” money to fund the activities of terrorists and their communities.

Identity Theft – what is it?

Identity theft and identity fraud can best be defined as “... the gaining of money, goods, services or other benefits or the avoidance of obligations through the use of a false identity...”. Identity fraud relates to the fraudulent use of either:

- A person’s personal details or
- A business’ details
- Company details or
- Even Government Dept details
- Local and foreign – there is no boundary

When you consider identity theft in this light, it is **NOT** a victimless crime as the false or stolen identity is being used to fraudulently obtain goods, services, shares or property and even the personality of the person or business used to perpetrate the fraud.

A false identity is created through the use of:

- Falsely obtained documents (i.e. can’t beat the “real thing”) or
- Forged / counterfeit documents – although with the added security features being added to key identity documents, these documents are becoming more difficult to copy / forge. For example:
 - Personal details can be obtained from birth certificates, passports, driver’s license, employment records and even academic records
 - Business details – registration / ASIC records / industry records

Managing your identity in the online world

The real issue facing online service providers and especially the financial services industry is the ability for a criminal or someone wishing to create a false identity need only look as far as the internet where identities can be bought and sold!

Identity Fraud

Within the banking industry and the broader online services community including online merchants, the risk of identity fraud is part of history and a risk faced both by the real and online businesses on a daily basis.



The use of fraudulent identities is most often attributed to:

- Criminals using the false or fraudulent identity to hide from the authorities;
- Terrorists using one or more false identities to avoid detection from the law enforcement agencies when moving around the world;
- A desire to avoid taxation and other government imposts through the use of fraudulent or false identities to hide income and investments from the taxation and revenue authorities – and the trend is growing;
- Hiding illegal and illegitimate activities from the authorities, individuals and the businesses with which they conduct business.

The ability for fraudsters to develop a fraudulent, false or stolen identity may become more difficult as authorities and online service providers strengthen the processes and procedures by which details of birth records, death records, company records and other public domain based records can be obtained and used for identification purposes.

However, the fraudsters are now tending to access the personal and sensitive business details with the sole objective of using this information to leverage someone else's identity to create a new identity for themselves and can achieve this by any one of a number of means including:

- Utilising the internet to search for or to obtain personal details and business details of the "target" and then building a profile based on internet sourced information;
- Using bogus emails to induce the recipient to act on the message and effectively provide their personal and often most private details;
- Creating "facsimile" versions of the genuine article using the information obtained from the internet and potentially other sources;
- Package the identity and sell over the internet;
- Personal, Business and Government are not immune;
- Even passports are not immune;
- Online commerce is only adding to the problem – customer not present.

The use of online services created by the fraudsters, to look and feel like the genuine web sites and online services is also being used to deceive innocent users to provide personal or sensitive

Managing your identity in the online world

business details. The very nature of these false sites and the realistic look and feel of the sites make it all the more difficult for the untrained eye to determine the difference between a “phishing” web site and the genuine web site. Ultimately we find that the fraudsters are able to entice personal and business customers of genuine internet services to unwittingly use these sites to provide information that we would not otherwise disclose if we knew the true identity of or the intention of the “phishing” web site.

Who is affected by Identity Theft / Identity Fraud

The underlying tenet of identity theft is to defraud either the owner of the identity or to use the identity to defraud:

- Another person or persons;
- Professionals such as lawyers / accountants / doctors / financial advisers etc.....
- Small and medium sized businesses;
- Corporate and institutional businesses;
- Banks and other financial service providers;
- International businesses;
- Governments at the local, state, federal and even foreign levels and;
- Even foreign nationals where the identity of a foreign national is used locally and often with the knowledge that the ability to verify and validate the identity is problematic as the source of identity may not be accessible or able to verify the authenticity of the identity documents offered.

Not only is the loss of property at risk as a result of the fraud, but the personal or business reputation and overall life and well being of the persons or businesses may be adversely affected to the extent that it may take considerable funds and time to re-establish their career, personal or business finances and credit ratings. Loss of income, loss of assets, friendships and business relationships along with credit ratings may result from such fraudulent activities.

Identity Theft – and the internet

The internet has opened the door to a wide range and variety of sources of sensitive and often private personal and business related information. The exchange of this information via the internet is usually conducted on the assumption or belief that the exchange is taking place in a safe and secure environment.

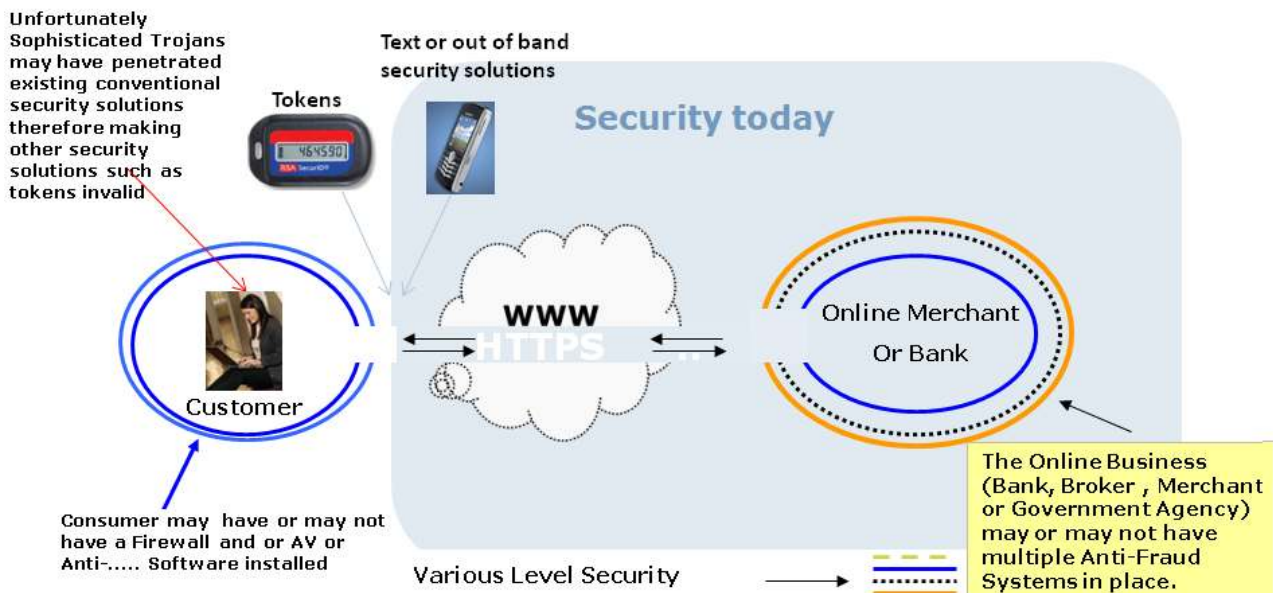
In addition to the provision of online services, the creation of social networking web sites and the need to provide business and investment details on company web sites has opened the door to potential use of this detail by the fraudsters.

Managing your identity in the online world

At the personal level, the rise of social networking website services such as Bebo, MySpace, Facebook, You Tube and LinkedIn are examples of where personal details are placed on the internet and can be seen and used by others. The level of security provided by the social networking websites is in most cases if not always substantially less than the security of financial institutions including the banks. In addition, personal details are often exchanged with online subscription based services that require users to provide personal and or confidential details. These details are at risk of being attacked through a phishing activity or database hijack with the sole purpose of gaining access to personal and often sensitive details for use in creating a false identity and then applying this identity to defraud the owner of the identity or others that rely on the identity.

To the untrained eye, the phishing web sites are as good as the genuine article and can convince the unwary user that their personal and most intimate details remain safe and secure. **It is often the case that the user is very familiar with a web site and may overlook the fact that a website has been substituted by a phishing web site, only to unwittingly provide their confidential details.**

Online security in theory should extend beyond the online service provider or enterprise to encompass the computing device of the end-user customer in real-time – but to date this has not been a priority as security solutions provided by traditional security vendors operate independently and are reliant on the customer updating the black list or heuristics regularly and paying an annual subscription fee – most end users fail to regularly update their security software and likewise most don't know their computing devices' security status. In addition online service providers such as banks provide security to the front door of the computer and do deploy token or text message security codes via a third party device but do not secure the computer from malware and man-in-the-middle attacks derived from the computer itself.



At the business level, business documents often used to establish the identity and bona fides of a business client, can also be established from records commonly recorded by and often posted on public and government web sites including:

Managing your identity in the online world

- Australian Securities and Investment Commission (ASIC)
- Australian Taxation Office (ATO)
- Australian Stock Exchange (ASX)
- Business and professional associations
- News web sites
- Business and trade magazines
- Business Who's Who
-

In short, the message is “..... **beware of where of the security status of the computer you are using and the security of the website you are visiting when you post business details on the internet!**”

The future

To guard against the potential creation of and use of false identities for fraudulent purposes or to disguise the activities of the fraudsters, online service providers including consumer and business users will need to ensure the information procured by the online service provider is and remains secured in an accredited data storage facility and that all online activity is conducted in a safe and secure environment.



However, the ability to control and to manage the identity of the individuals and businesses alike will have a dependency on:

- the physical presence of the customer or the identity management media (Personal and Business Customers alike);
- the presence of the individual (includes business related activities);
- the creation and operation of a repository of “genuine” samples for verifying the authenticity of a document or person e.g. establishing an Identity Clearing House;
- facilitating the greater disclosure to track and monitor ID fraud and the reporting of the related crime(s) or activities to the appropriate authorities and;
- Build the case for legislative measures to manage the citizen identity.
- Developing end point security solutions that provide a security envelope that covers the end user computing device, the online service provider, all information transacted and the overall links between the end user and the online service provider.

Identity Management – an imperative

As the legislative framework in Australia and around the world tightens the reins on regulatory compliance, anti-money laundering and counter terrorist financing related activities, there is a growing need to ensure that the information collected by online services providers including

Managing your identity in the online world

merchants, banks and government agencies remain secure at all times. In addition there is a requirement that these service providers have the appropriate systems in place to enable them to not only understand their customer's security health status but, where appropriate, inform the customer of their security health status and to provide the tools to secure the customer's confidential information before and during any online transaction, especially applying policies and rules based on the customer's low, medium or high risk status.

A key area that would suggest that the customer is a high risk is where the customer acts outside their normal profile, such as using a computing device that is compromised by malware or has potentially dangerous unknown application(s) running, or where the customer attempts to make a transaction from an unknown device located in an overseas location one minute and another overseas location the next. In these instances the online service provider, the merchant or the financial institution must remain alert and vigilant to possible variations in a customer's behaviour which may suggest that the activity is fraudulent or may suggest that anti-money laundering/counter terrorist financing type activity is being undertaken. Detecting such changes in customer behaviour or where the device being used may be compromised, in the first instance is not easy and is akin to finding the right needle in a haystack, when there is more than one needle in the haystack at any one time!

At a corporate level, with the increased level of regulatory and compliance activity in relation to online fraud and anti-money laundering / counter terrorist financing related activities, the ability to carry out fraudulent activities without being detected by the authorities is diminishing, however consumers and small business need to employ best practice security technologies and methodologies to stay ahead of the online criminal.

Further, as the legal and regulatory framework tightens, the criminals who undertake these activities are finding it difficult to hide from the authorities. But the online criminal is smart and will pursue alternative paths to exploit the weaknesses in the systems used by consumers, business and the financial services providers to their own advantage – which includes using false or stolen identities to hide their activities from the authorities and from the banks and financial service providers – who are most often the key targets of their activities.

From the viewpoint of a bank, a financial services provider or even the online service provider such as a merchant and even the authorities, the emphasis is to not only monitor the transaction activities of their clients for suspicious or potential anti-money laundering or terrorism financing related activities in a broader sense, the service provider must also be vigilant in detecting possible fraudulent activity related to the use of fraudulent or stolen identities – both at a personal level and non-personal or business level.

Fraud not only affects monetary transactions but, as noted previously, it also affects the well being of the individual or business or both in terms of the loss of their privacy but also the potential financial and other non-monetary losses that may result from the fraud.

Managing your identity in the online world

Managing your identity in an online world

The growth in online commerce and the increased use of online services creates the potential for a person's identity to be stolen or to be used by another whose key objective is to use the identity to hide their illegal activities or to disguise their activities in such a way as to prevent early or easy detection. The need to use a genuine identity over a falsely created identity also serves a purpose for those using a stolen identity in that the genuine identity is used to also delay the detection of the activities of the perpetrator – to the extent that even general credit card fraud, money laundering, terrorist financing and other illegal activities are made harder to detect.

Whilst we appreciate the convenience and efficiency of using the internet to manage our day to day affairs, online services are only as safe if the service provider **and** the end user adopt a complete and full end-to-end or end point security solution that secures the end user's computer **AND** provides the security over the entire internet session – from end user to the service provider's own service.

In the online world, there is the need for a true end-to-end or an end point security solution that integrates the PC or mobile computing device into the overall security chain or creates a secure envelope with the online service provider or institution. This secure envelope is a requirement that is the key to ensuring that all information that is exchanged online, including invaluable personal identity details and passwords, remain secure and cannot be intercepted at any point along the transaction or information stream.

To ensure that our personal and private details including passwords and security text codes or token codes remain secure, including all content in the transactions we conduct online remain safe and secure, there is an imperative that we use the internet for personal and business purposes with the full knowledge that our personal, financial and private details remain secure and uncompromised throughout the period of each online session, away from the prying eyes of a criminal or third party activities. Always remembering the criminal or third party's sole purpose is to access your personal details, including your identity, for their own gain – and to the detriment of those who rely on the safe and secure exchange of information.

How we prevent the loss of your identity in a material world

Managing your identity is paramount to maintaining your life style, relationships, career and personal finances. Lose your identity and you risk the loss of your personal and business assets, relationships and potentially suffer the indignity of having a poor credit rating or even a criminal record that is the result of the activities of the person(s) who have accessed your identity details for their own gain.

In the offline world, there are some simple measures we can take to secure our identity and to ensure that our identity details are only available to those who have a genuine need to access your personal or business details including banks, insurance companies, employers and

Managing your identity in the online world

government agencies. More importantly, when disposing of any documents that contain personal details, it is an imperative that every effort is taken to obliterate the identity details from these documents and the best approach is to destroy or shred these documents – even when recycling paper based materials to prevent the details falling in to the wrong hands when they enter the recycling services. It is also important to monitor mail deliveries to ensure that regular bills, statements and other correspondence that may contain personal details always arrives safely, as a loss of mail may indicate that mail is being intercepted or rerouted without your knowledge or approval – and this can be the first sign of a potential identity based fraud as information is now flowing to the fraudsters or those with fraud or money laundering on their minds.

Managing online security – there is no compromise

As is with the offline world, in the online world managing your identity is even more complex. It is important that your identity is protected at all times if you wish to maintain your current life style, relationships, career and personal finances. Lose your identity online and you risk the loss of your personal and business assets, relationships and potentially suffer the indignity of having a poor credit rating or even a criminal record that is the result of the activities of the person(s) who have accessed your identity details for their own gain.

In order to protect our identity, we must ensure that any personal details including passwords, ID's and even the security codes provided independently by text or token and by a third party device are not shared or made available to a person or business without understanding the intended use of the personal details.

Typically, the use of physical forms of personal identification including passport, driver's license, birth certificate, bank statements, credit cards and other accredited forms of identification are relied upon to open and to operate bank accounts, establish insurance policies and to satisfy general requests for identification. In the online world, these forms of identification are rarely if ever required to substantiate the identity details provided to an online service provider. This creates the opportunity for online identity fraud as it is difficult to verify and to validate that any personal details that are provided over the internet are being used by the intended end user and not by another party who has managed to access their personal or business details through a back door attack on their personal computer – at home or even at the office.

To resolve the risk of exchanging information with a potential fraudulent user, on line service providers and their clients – both personal and business – need to use an On-Demand Endpoint Security solution that verifies the security health of the computer you are using, enables ease of use and enable easy rectification where a security fault may occur and is able to apply security policies that secure your computer whenever a transaction takes place. In order to accomplish this, the solution needs to be on-demand and applies all the five security factors that will provide a comprehensive and effective way of providing a general trust solution to all Online Fraud Issues.

Managing your identity in the online world

The five factors comprise:

Authentication

A user of an Online Business has first to be authenticated. The most common method today is the one factor authentication (e.g. username and password). Two-factor Authentication is more and more common for high end security Applications.

Access Control

The Access Control defines Policies of who is allowed to request and access an Online Service. This Policy can be applied to all of the Five Sections and includes e.g. Policies of how the end user's Computer has to look like in order to proceed with the Online Transaction. Obviously the Identity is also part of the Access Control.

Trust Policies

The Trust Policies defines exactly which Components have to be trusted in order to complete the Online Transaction. These can include Hostnames, SSL Certificates, but can also be applied to the other sections and can include the Identity or Internet Access Policies like Geo-IP.

System Policies

The System Policies will include Policies based on the overall Topology and different Policies can be applied e.g. based on VPN Access.

Network Policies

The Network Policies defines Policies who/when/what User/Software is allowed to request either the Internet of a specific service. This Policy can include e.g. a sophisticated Personal Firewall blocking Internet Requests to non-related Sites only during an Online Transaction.

Identity Theft, Brand Protection and Customer Loyalty

The impact of a secure end-to-end security solution, which also serves to ensure the security and the integrity of the end user's identity can simply be put down to three key factors:

1. It serves to protect the Internet user from fastest growing crime;
2. It provides a high level of security over the full end-to-end transaction, extending the overall security chain beyond the enterprise to the end-users computer and information exchange is secure, ensuring the Brand Protection for all online service providers who deploy and use a true end point security solution and,
3. It creates a higher level of customer loyalty for growing Brands by return growth business.

Managing your identity in the online world

About the Author

Peter Ager is an experienced Banker and Finance Sector Solutions Architect with over 30 Years experience in the finance industry, specialising in compliance, systems design, implementation and remediation. Peter's experience extends to development of leading edge technology solutions in the finance sector, public health and government business both in Australia and in global markets.

Peter has held senior technology and compliance roles within the Commonwealth Bank, Westpac Bank, Hewlett Packard, PWC and Colonial Bank. In recent times he chaired the Bankers AML/CTF working committee in Australia dealing with compliance and meeting legislative requirements.

Today Peter continues to provide consultative input to the Bankers AML/CTF working committee and is a member of the TrustDefender advisory board.

About TrustDefender

TrustDefender™ (Symbiotic Technologies Pty Ltd) is an award winning Australian owned and operated privately held company headquartered in Sydney, NSW. The company was established in December, 2005 after over two years of research and development into the global issue of growing online fraud in the online community - with a focus on 'hardening' the security at the PC and growing number of mobile computing devices entering the market.

Research and development was based on identifying the weaknesses in the overall security chain between Business to Consumer (B2C), Business to Business (B2B), Government to Consumer (G2C) and Government to Business (G2B) - where online criminals can penetrate the integrity of the user's confidential information before and during an online transaction.

TrustDefender™ has developed a world first security solution that can be applied as an Enterprise Server solution or utilised as a managed service or independently by consumers using their home PC or mobile computing device. TrustDefender™ authenticates the security health status of the end user computer whilst extending beyond the security of the enterprise environment.

TrustDefender™ was set up with a global focus in provisioning 'On-Demand Endpoint Security Solutions' for banks, financial institutions, government, online merchants and for consumers in general.

TrustDefender™ is a member of the 'UN Global Compact' adhering to corporate social responsibility guidelines.

