Executive Summary

Phishing is the new 21st century crime. Globally, the stories are covered by almost all international media covering the latest organisation to have their customers targeted and how many victims succumbed to attacks. Phishing is an online identity theft in which confidential informations are obtained from an individual. Phishing includes deceptive attacks, in which users are tricked by fraudulent messages into giving out information, malware attacks, in which malicious software causes data compromise, and DNS (Domain Name System) based attacks, in which the lookup of host names is altered to send users to a fraudulent server.

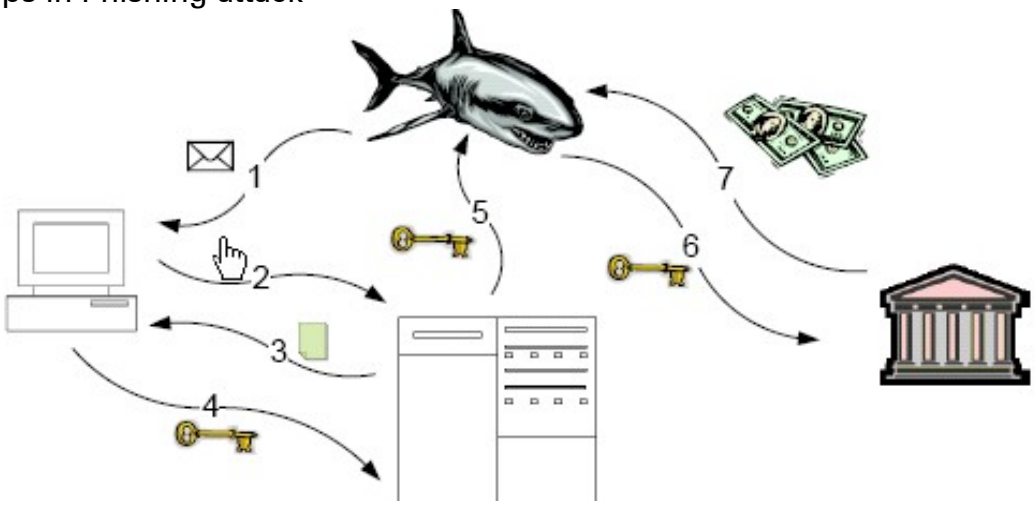
There is no precise estimation of losses due to phishing, however the Gartner group estimates that the total financial losses attributable due to phishing for US Banks will be approximately US$ 2.8 billion for the year 2006. The indirect losses are much higher, including customer service expenses, account replacement costs and higher expenses due to decreased use of online services in the face of widespread fear about the security of online financial transactions.

This report cover the countermeasure implemented by various foreign banks against phishing, informations that are available in public domain.

Harish Kesharwani

CA.Grad CWA, M.Com

Steps in Phishing attack[1]



All phishing attacks fit into the same general information flow. At each step in the flow, different countermeasures can be applied to stop phishing. The steps are:

0. The phisher prepares for the attack. Step 0 countermeasures include monitoring malicious activity to detect a phishing attack before it begins.

1. A malicious payload arrives through some propagation vector. Step 1 countermeasures involve preventing a phishing message or security exploit from arriving.

2. The user takes an action that makes him or her vulnerable to an information compromise. Step 2 countermeasures involve detecting phishing tactics and rendering phishing messages less deceptive.

3. The user is prompted for confidential information, either by a remote web site or locally by a Web Trojan. Step 3 countermeasures are focused on preventing phishing content from reaching the user.

4. The user compromises confidential information. Step 4 countermeasures concentrate on preventing information from being compromised.

5. The confidential information is transmitted from a phishing server to the phisher. Step 5 countermeasures involve tracking information transmittal.

6. The confidential information is used to impersonate the user. Step 6 countermeasures center on rendering the information useless to a phisher.

7. The phisher engages in fraud using the compromised information. Step 7 countermeasures focus on preventing the phisher from receiving money.

[1] Content taken from Report Title – Online Identity Theft: Phishing Technology, Choke points and Countermeasures available in website

Table of Contents

1. Abstract

As more and more systems are getting connected to the Internet, the risk of system attacks by malicious users is also increasing. Most of the services are becoming online these days. Nowadays one can make transactions with financial institutions and shopping marts just with a click of the mouse. Phishing is a form of cyber attack in which scammers make internet users divulge their sensitive information about their bank accounts and personal details. The scammers are able to target internet users due to some inherent weakness in web browsers and other technical aspects of the Internet. The solution to this problem lies in taking countermeasures at financial institution and at the end user levels.

2. Introduction

In computing, phishing is a criminal activity using social engineering techniques. Phishers attempt to fraudulently acquire sensitive informations, such as passwords and credit card details by sending impersonated fraudulent e-mails and web pages. In a typical phishing attack a user will receive an e-mail message impersonated to be sent by a financial institution. The e-mail will carry the spoofed image or logo of the financial institution and convince the user to provide personal and account details by means of visiting a web link given in the message. When a user clicks the web link a malicious web page, which is exact replica of the financial institution and actually hosted by the fraudsters, is opened. A normal user unaware of such malicious activity in turn provides his/her personal and account details to the fraudsters. The phishers use this information for fraudulent use amounting to financial gains. Phishing attack involves fraudulent message sent to thousands of users or even more in an attempt that atleast a small percent of users will respond.

Pharming is a technique to redirect users from real websites to the fraudulent websites by using malware/ spyware. Pharming uses modification in name resolution system, so as when a user clicks a financial institution web page, it actually goes to spoofed website.

3. Phishing attack

There has been significant rise in the phishing attack during recent pasts. Phishing attacks are also combined with malicious code attack like Trojans. In such blended attacks these virus/ worms carry the viruses which harnesses e-mail addresses from the internet and affected systems and further launch phishing attacks.

3.1 Phishing trends

The Anti-Phishing Working Group (APWG) is the global pan-industrial and law enforcement association focused on eliminating fraud and identity theft that result from phishing, pharming and email spoofing of all types. The group provides a forum to discuss phishing issues, trials and evaluations of potential technology solutions, and access to a centralized repository of phishing attacks. The group is publishing Phishing Site Outbreak Report on a regular basis. The highlights of Phishing Site Outbreak Report October, 2006 are mentioned below :

- Number of unique phishing reports received in October 26877
- Number of unique phishing sites received in October 37444
- Number of brands hijacked by phishing campaigns in October 176
- Number of brands comprising the top 80% of phishing campaigns in October 18
- Country hosting the most phishing websites in October United States
- Average time online for site 4.5 Days
- Longest time online for site 30 Days

4. International Scenario

The trends of phishing attack dates back to 1996 when the first phishing attack was on American Online Limited (AOL) accounts by hackers, to steal passwords from AOL users. Over a period of time phishing attack has taken varied faces like Spoofed email, Malware based phishing , Key loggers, Screen loggers, Man-in –middle phishing, Data Theft, Web Trojans, Pharming, Sessions Hijackers etc. The type of phishing and the method of phishing attack evolve every day.

Various groups like Anti Phishing Working group, governments and private financial organisations are actively involved in preventing damages due to phishing attacks.

US government has passed a legislation called Anti-Phishing Act in the year 2005. The UK has also passed similar act called Fraud Act 2006. Various other governments have recognized phishing as a type of sophisticated criminal fraud and have taken steps to punish the guilty.

The US government has even started a dedicated website to create awareness among the people for phishing and identity theft.

As per Gartner Group, the average loss per phishing attack was $ 1244 during the year 2006, up from the average loss of $255 last year in US alone. Estimated total financial loss to be around $ 2.8 billion for year 2006. The recovery percentage has decreased during the year 2006 and is around 54% down from 80% a year back.

A number of international banks have iniated various countermeasures to protect their customers from phishing attacks. The general steps taken by various banks are focused on customer awareness, technological changes of their online platform and recommendation of use of anti-viruses etc.

The report outlines the initiatives taken by various banks around the world to protect their organisation, customers and people at large from phishing attacks.

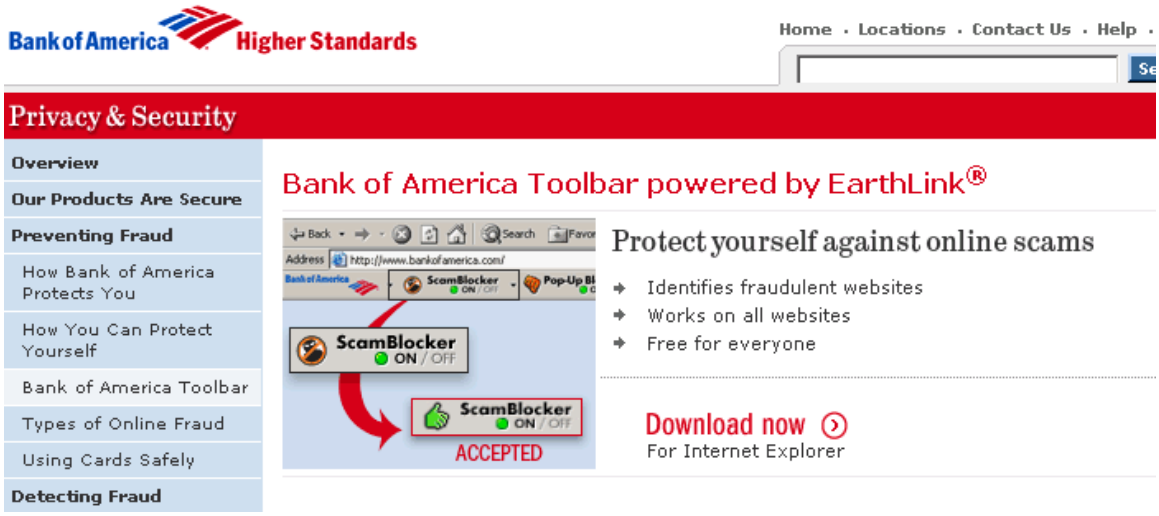
4. 1 Bank of America.

Bank of America the No.7[2] bank in the world in terms of asset size, has taken the following steps to prevent online frauds and phishing:

1) Anti – Phishing toolbar to all customers at no cost.
2) First Level of authentication known as SITE – Key.
3) Zero Liability guarantee for unauthorized online transaction.

4.1.1 Anti – Phishing toolbar to the entire customer at no cost.

Bank of America provides Anti-Phishing Toolbar to all their customers, which if installed by the customer in their computers helps in identifying the genuinity of the website browsed by the customers.



Features of Bank of America Toolbar are:

- Displays a security rating for every website the customer visits
- Alerts customers before customers enter a website on a list of known fraudulent sites
- Includes EarthLink's innovative Pop-Up Blocker™ tool

The Toolbar's ScamBlocker™ feature alerts the customers to “phisher” websites – fraudulent sites that mimic legitimate bank, auction, or internet payment sites in an attempt to steal credit card number, social security number, pass codes or identity.
The indicators of the tool bar are:

[2] As per published report in bankersalmanac.com website

- A red “thumbs down” in the toolbar - means that the website is potentially dangerous and the customers shouldn't provide the site with any of their personal informations.
- A yellow “thumbs down” - means the website is questionable.
- A green “thumbs up” means a website is safe.
- A “shadow” icon means the website doesn't appear fraudulent.

The use of the Toolbar in conjunction with a personal firewall and anti-spyware and anti-virus protection, gives an added level of online protection.

4.1.2 Site Key.

Bank of America has implemented “ Site Key” features as a part of online login to internet banking, which provides an extra level of authentication.

The process:

Customers pick one of thousands of images, write a brief phrase and select three challenge questions. The customer and the bank can pass that information securely back and forth to confirm each other's identity.

Customers can register their computer, hence when a customer login through a registered computer, the images are shown. If customer logs in from any other computer, any of the three-security questions will be asked. Please refer page 37 for detailed login process.

4.1.3 Zero Liability guarantee for unauthorized online transaction.

The bank provides 100% refund of losses due to any unauthorized online transaction in the customers account.

4.2 The Hong Kong & Sanghai Banking Corporation.

HSBC bank the no. 21[3] bank in the world in terms of asset size, has taken the following steps to prevent online fraud and phishing:

1) HSBC – Security device.
2) Customer awareness - 5 golden rules.

4.2.1 HSBC – Security device.

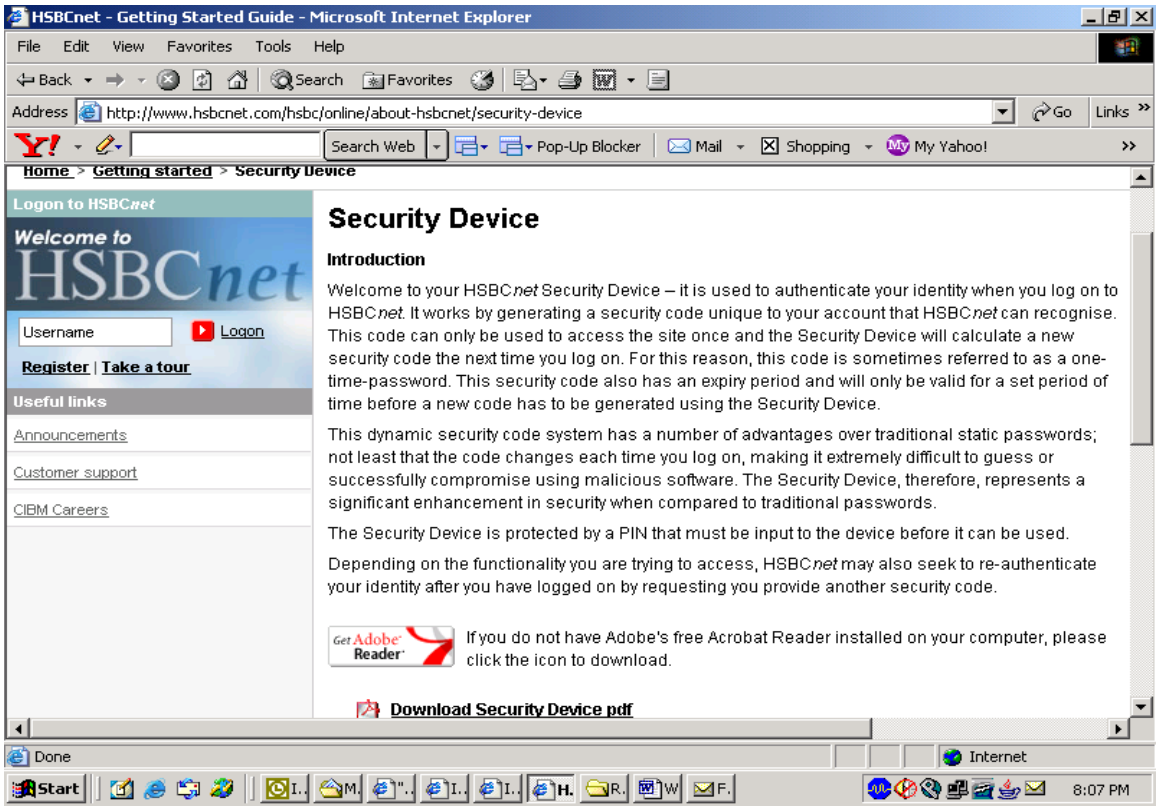
[3] As per published report in bankersalmanac.com website

HSBC Security device is used to authenticate the identity when any customer logs on to HSBCnet, the internet banking portal of HSBC. It works by generating a one-time security code (one time password) unique to a customer's account that HSBCnet can recognise. The code can only be used to access the site once and the security device calculates a new security code the next time the customer logs on. The code is also referred to as a one-time-password. This security code also has an expiry period and will only be valid for a set period of time before a new code will be generated using the Security device.

This dynamic security code system has a number of advantages over traditional static passwords, code changes each time the customer logs in, making it extremely difficult to guess or successfully compromise using malicious software.

The Security device, therefore, represents a significant enhancement in online security as compared to traditional passwords.

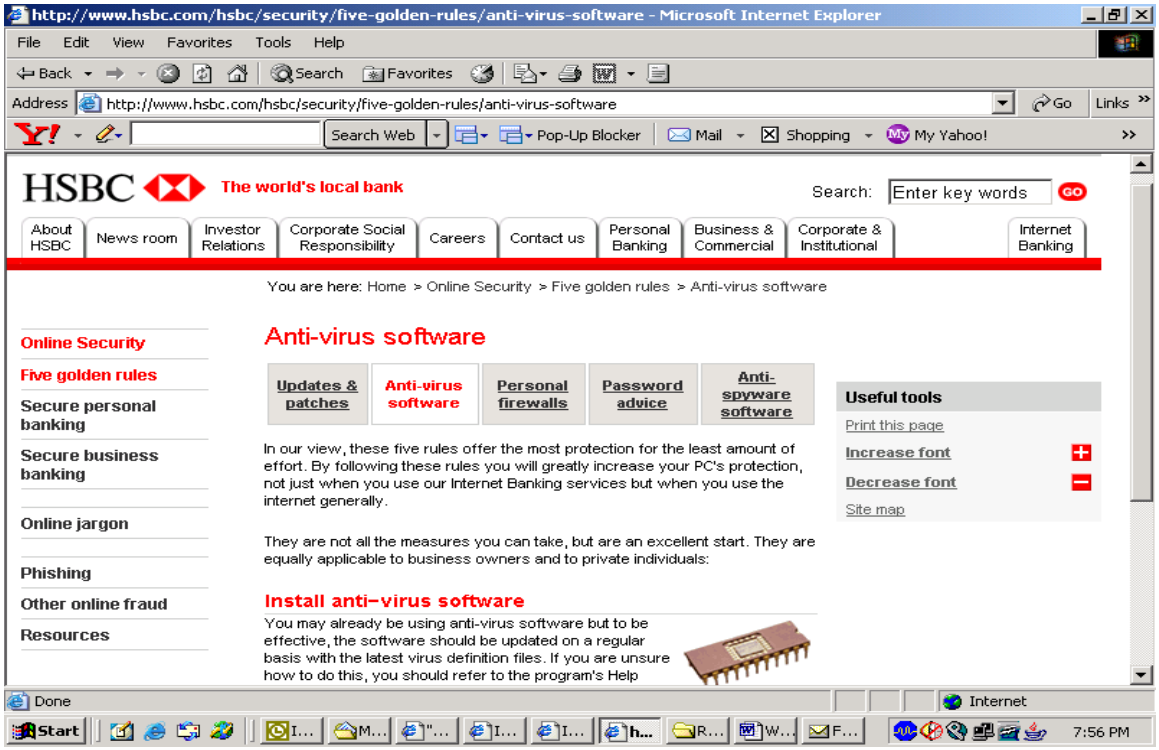
The Security device is also protected by a PIN that must be entered into the device before it can be used.



4.2.2 Customer awareness - 5 golden rules.

HSBC displays prominently on its website (www.hsbc.com) the 5 Golden Rule to be followed by customers for online security. The 5 Golden Rules are:

1. Latest Security updates & patches.
2. Installation of anti-virus software.
3. Use of personal firewall.
4. Password advice.
5. Anti Spam spyware.



In addition, the site also displays steps taken by HSBC Bank to protect online identity theft fraud and the steps customers should take to prevent the same.

4.3 US Bank.

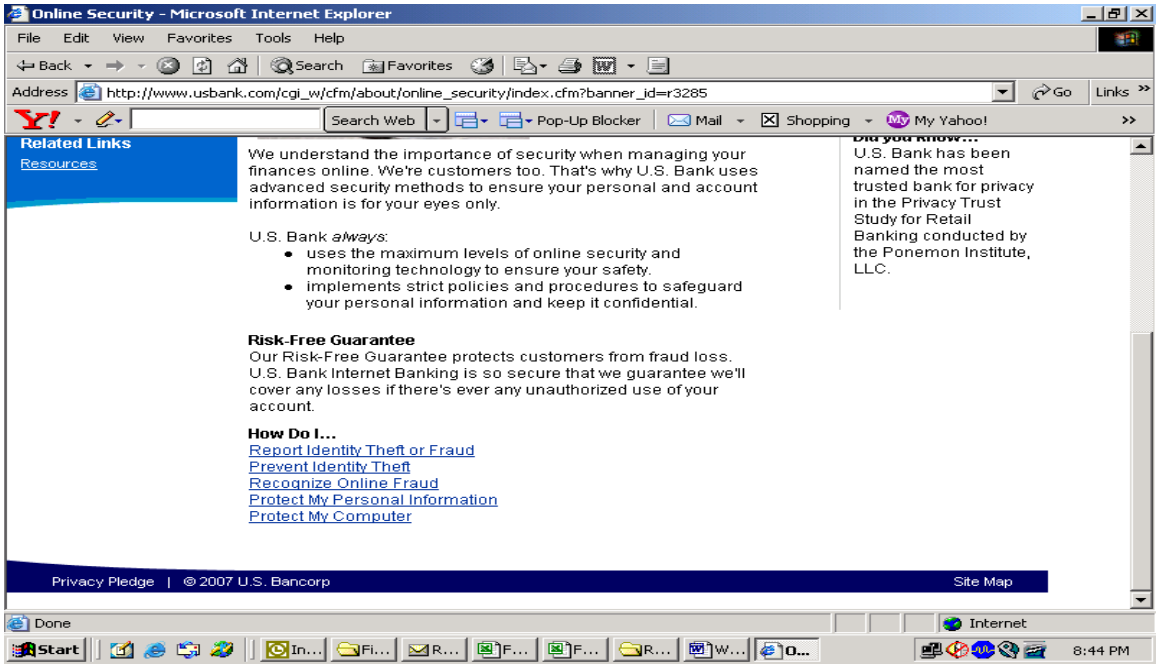
US bank the No.6 [4] bank in the world in terms of asset size, has taken the following steps to prevent online fraud and phishing:

1) Risk - free guarantee.
2) Customer awareness - E Newsletter.
3) Recommendation to download Security Patches of Microsoft.

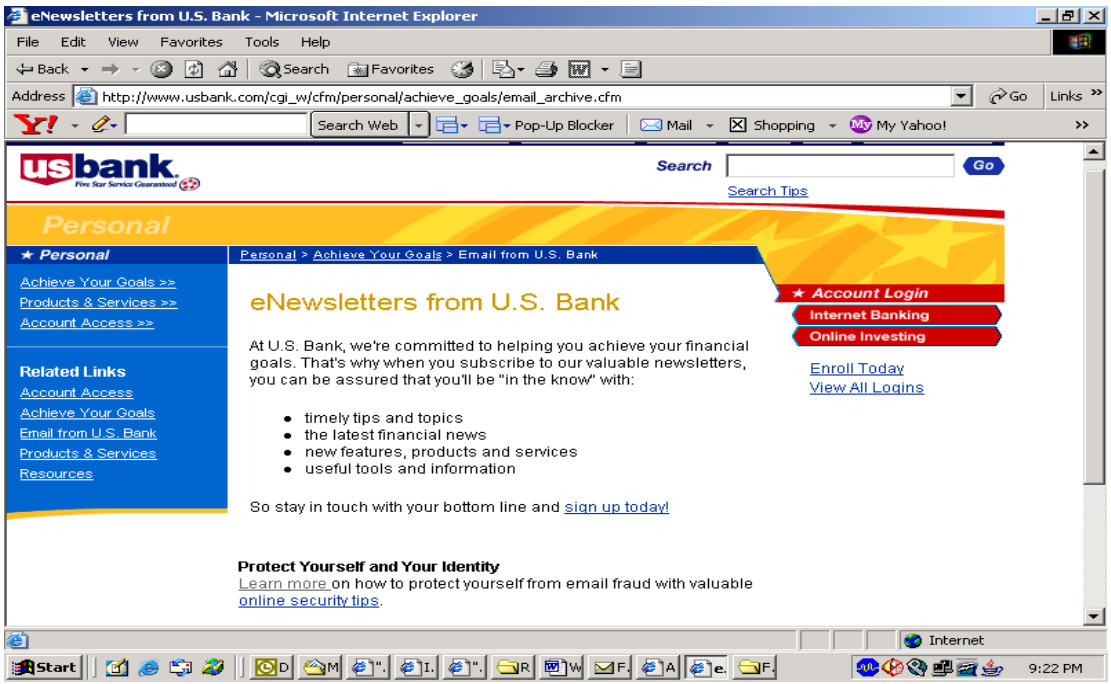
4.3.1 Risk –Free Guarantee.

[4] As per details provided in US bank website

U.S. Bank displays prominently on its website a risk free guarantee to all their customer, which covers losses from any unauthorized use of the customers accounts.

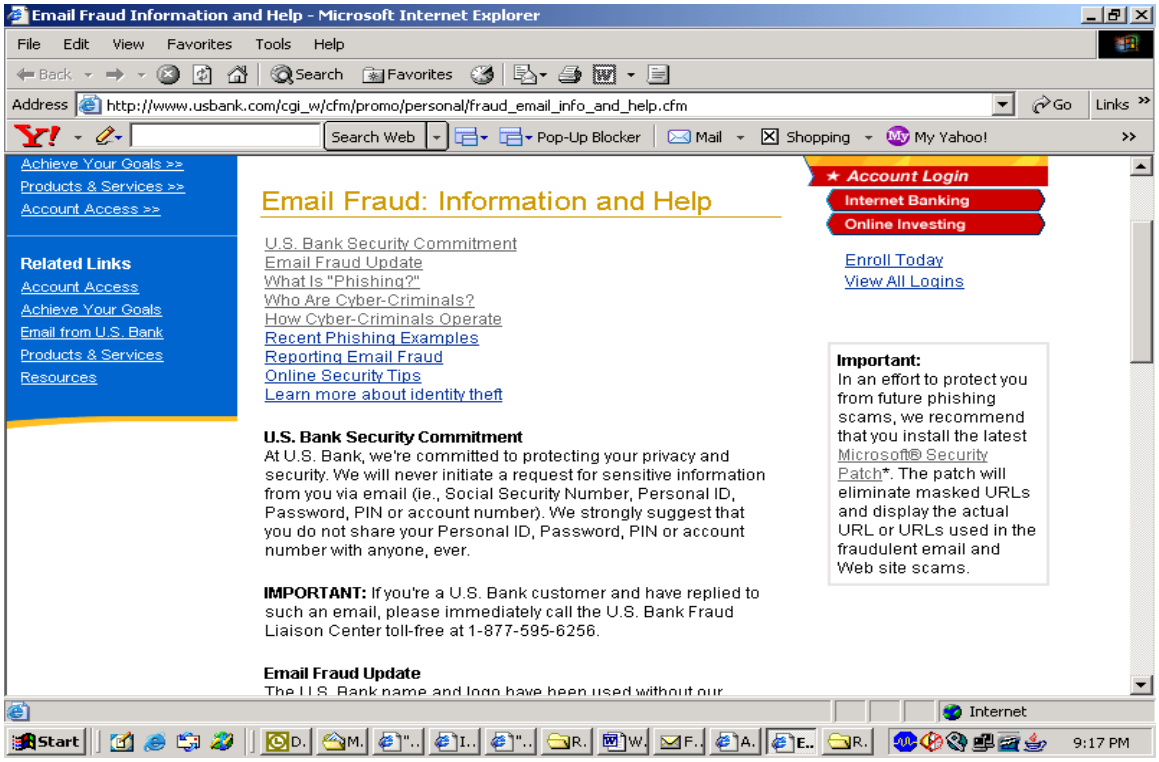


4.3.2 Customer awareness - E Newsletter.



4.3.3 Recommendation to download Security Patches offered by Microsoft.

US Bank advises all their customers to download security patches offered by Microsoft, which eliminates masked URLs and displays the actual URL or URLs used in the fraudulent email and Web site scams.



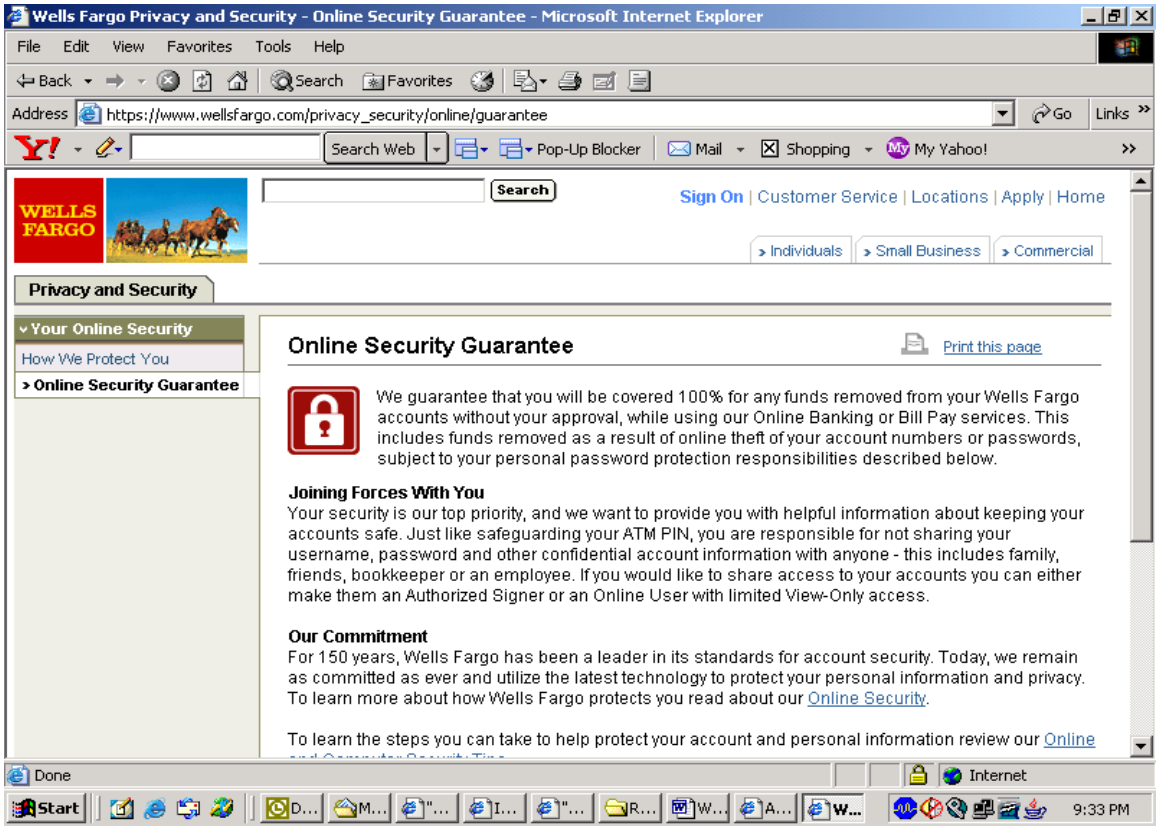
4.4 Wells Fargo Bank.

Wells Fargo bank the no. 40[5] bank in the world in terms of asset size, provides online security guarantee to prevent online fraud and phishing.

4.4.1 Online security guarantee.

Wells Fargo Bank provides guarantee to all their customers covering 100% for any funds removed from customers account in Wells Fargo account without the customers approval, while using Online Banking or Bill Pay services. The guarantee includes funds removed as a result of online theft of customer account numbers or passwords, subject to customer password protection responsibilities.

[5] As per published report in bankersalmanac.com website



4.5 Nat West bank.

Nat West (Part of The Royal Bank of Scotland Group) Bank the no. 4[6] bank in the world in terms of asset size, has provided Anti-Virus software at 32% discounts to all its customer to prevent online fraud and phishing.

4.5.1 Anti-Virus software at discounted price.

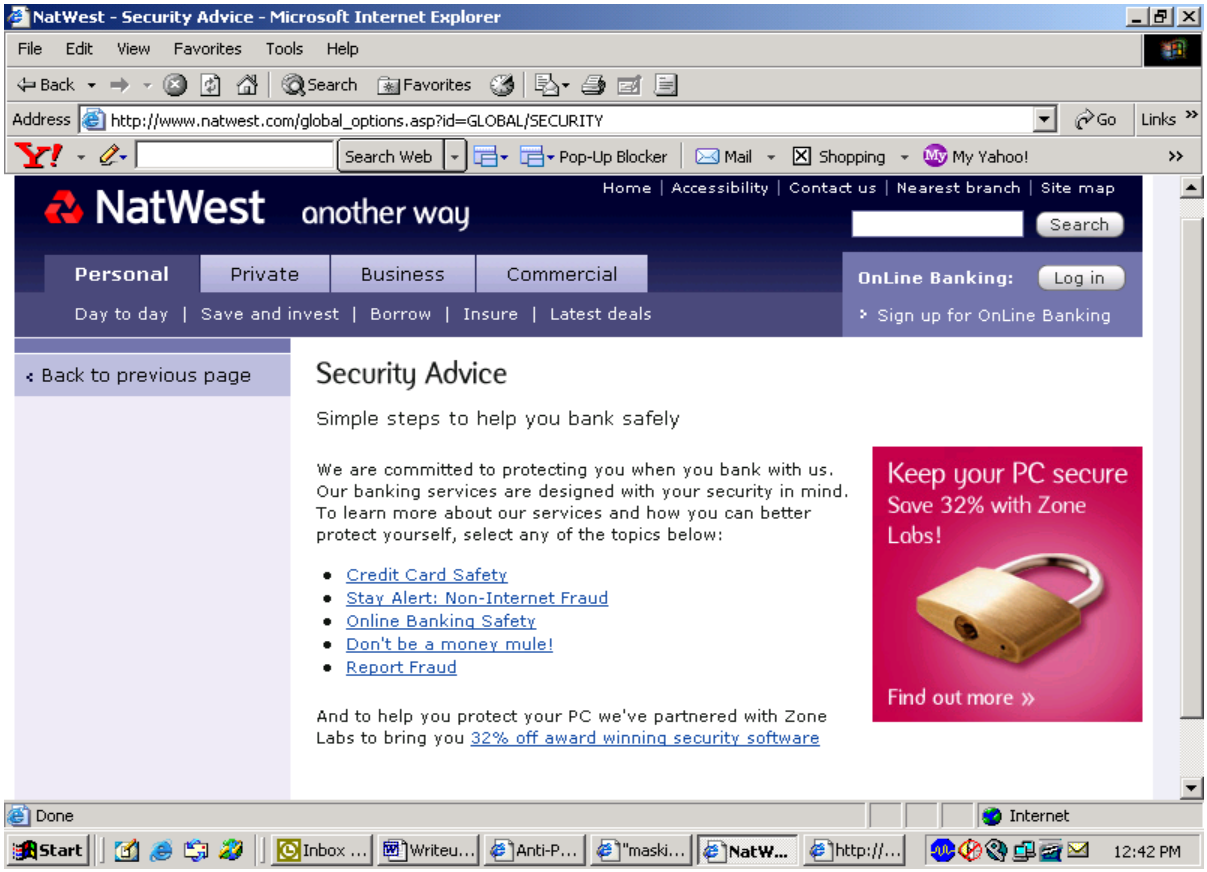
Nat West Bank as part of its online security features provides anti-virus software at discounted prices to all its customer.

The features of anti-virus software are:

- Fire wall Protection - protects from hackers, spyware, and other internet threats.
- Integrated Anti-Spyware and Antivirus updates.
- Real-time security updates and new attack protection capabilities.
- Identity and Privacy Protection.
- Email Security - quarantines suspicious email attachments and blocks outbound messages containing potential viruses.

[6] As per published report in bankersalmanac.com website

- Phishing and Spam Blocker.



4.6 eBay & PayPal.

eBay is the world's online marketplace, enabling trade on a local, national and international basis. eBay has a diverse and passionate community of individuals and small businesses. eBay offers an online platform where millions of items are traded each day. Millions of items are traded and paid online through Paypal, an online payment solution that claims to have over 100 million accounts as on date and increasing. Ebay has taken the following steps to help the online customers of eBay & Paypal to protect them from phishing and identity thefts.

4.6.1 eBay Toolbar.

eBay recommends that all their registered users use eBay toolbar. The toolbar apart from keeping a track of buying and selling activities of the users also provides the Account Guard protection. The Account Guard helps to prevent users from providing the eBay account information to any spoofed or phished websites.

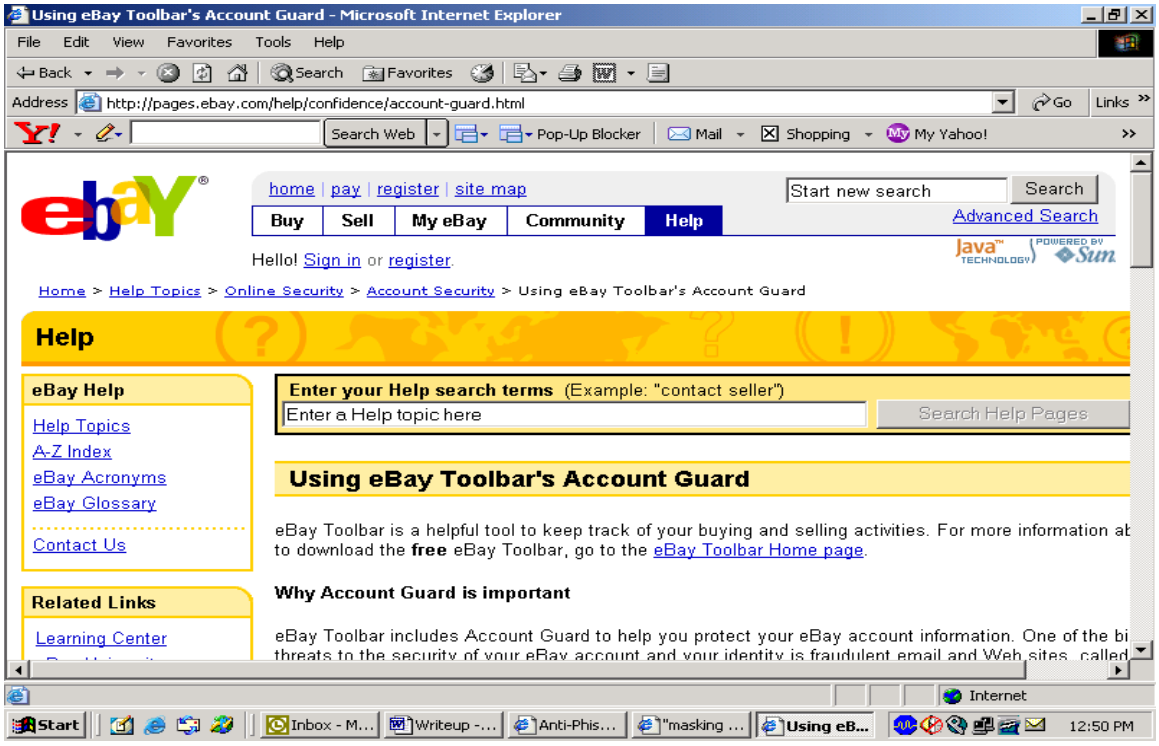
The features of Account Guard are:

1) Warns the user whether they 're on a potential spoof web site.

It has a Site Indicator on the eBay Toolbar that changes the color of the Account Guard button that indicates whether the user is on a verified site or a potential spoofed web site. Account Guard identifies only eBay and PayPal spoof web sites.

The Site Indicator turns:

Green if you are on a verified eBay or PayPal web site.
Red if you are on a potential spoof web site.
Gray if you are visiting an unidentified web site.



2) Provides eBay Password Protection.

It warns the users when they are entering eBay password into an unverified site (even if it looks like an eBay or PayPal site), and blocks eBay password from being submitted to the web site unless you affirm that you want to use your eBay password on that site.

3) Report spoofed web sites to eBay

If a user suspects any fraudulent (spoof) eBay or PayPal web site, the user can use the eBay Toolbar to report the site to eBay.

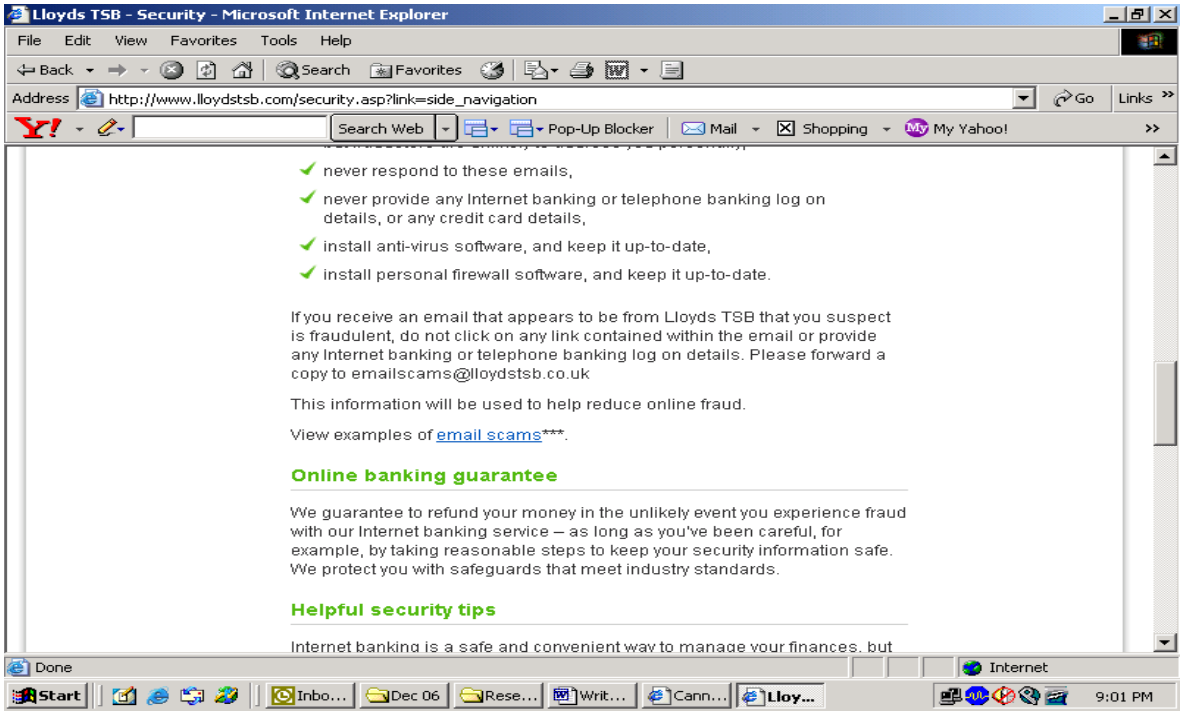
4.7 Lloyds TSB bank.

Lloyds TSB Bank the no. 30[7] bank in the world in terms of asset size, has taken the following steps to prevent online fraud and phishing:

1) Online banking guarantee.
2) Anti-Virus software at a discount to all their customers.

4.7.1 Online banking guarantee.

Lloyds TSB Bank provide guarantee to refund money to customers in the event of fraud with their internet banking service. The condition is that customers have to be careful and take reasonable steps to keep their personal online banking information safe.



4.7.2 Anti-Virus software at a discount to all customers.

[7] As per published report in bankersalmanac.com website

Lloyds TSB Bank advises all its customer to install anti-virus software for protecting their PCs from spyware and malicious attacks. The bank has tied up with an anti-virus software company and provides the software at a discounted price to all its customers.

4.8 Barclays Bank.

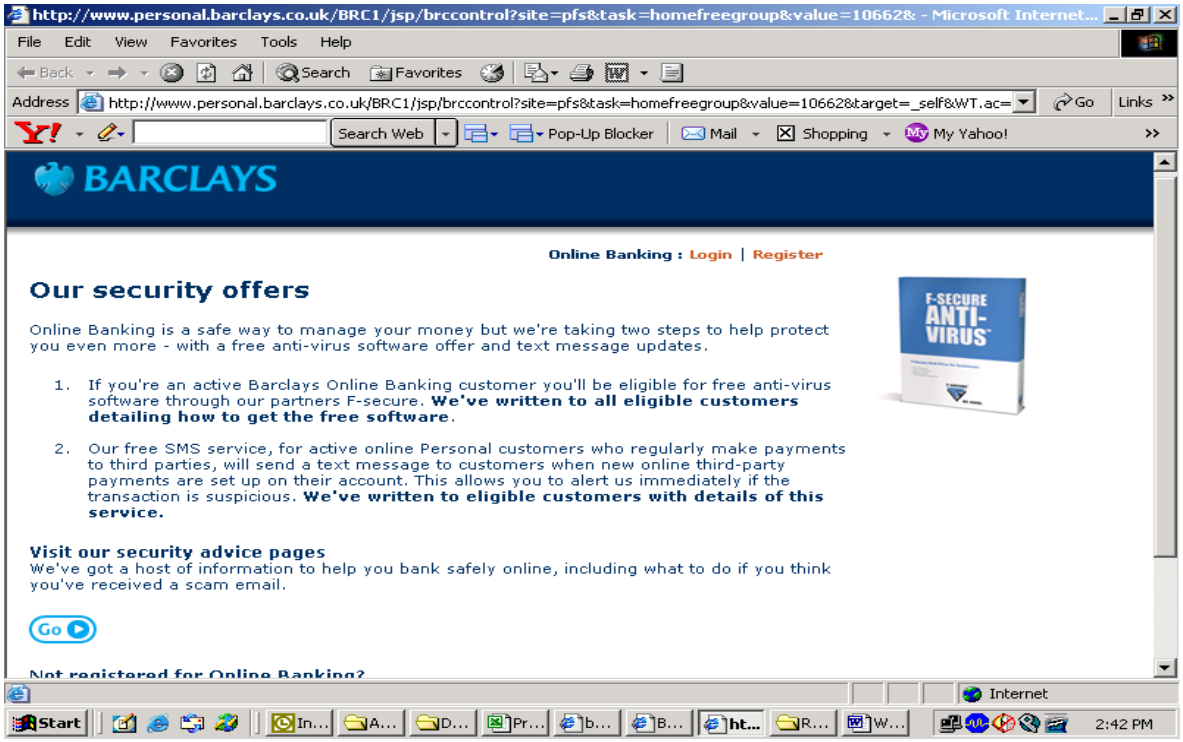
Barclays Bank the no. 1[8] bank in the world in terms of asset size, has taken the following steps to prevent online fraud and phishing:

1) Anti-Virus software free to all its customers.
2) SMS service
3) Multiple log-in process.
4) Online shopping verified by VISA.

4.8.1 Anti-Virus software free to all their customer.

Barclays Bank advises all its customers to install anti-virus software, to protect them from spyware and malicious attacks. The Bank provides the software free of cost to all their active online banking users.

[8] As per published report in bankersalmanac.com website



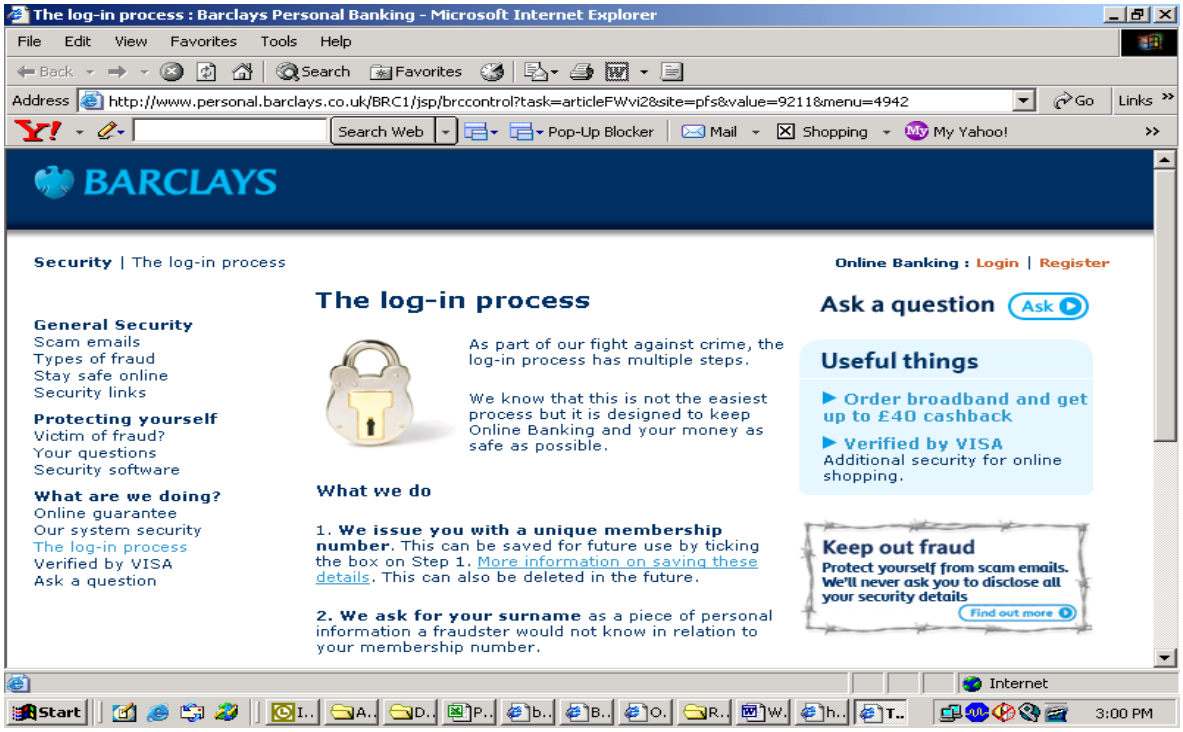
4.8.2 SMS services.

Barclays Bank offer SMS service, to all their active online personal customers who regularly make payments to third parties through online medium. Bank sends a text message to customers when new online third-party payments are set up on their account. This allows customer to alert the Bank immediately if the customer feels the transaction is suspicious.

4.8.3 Multiple Log-in process.

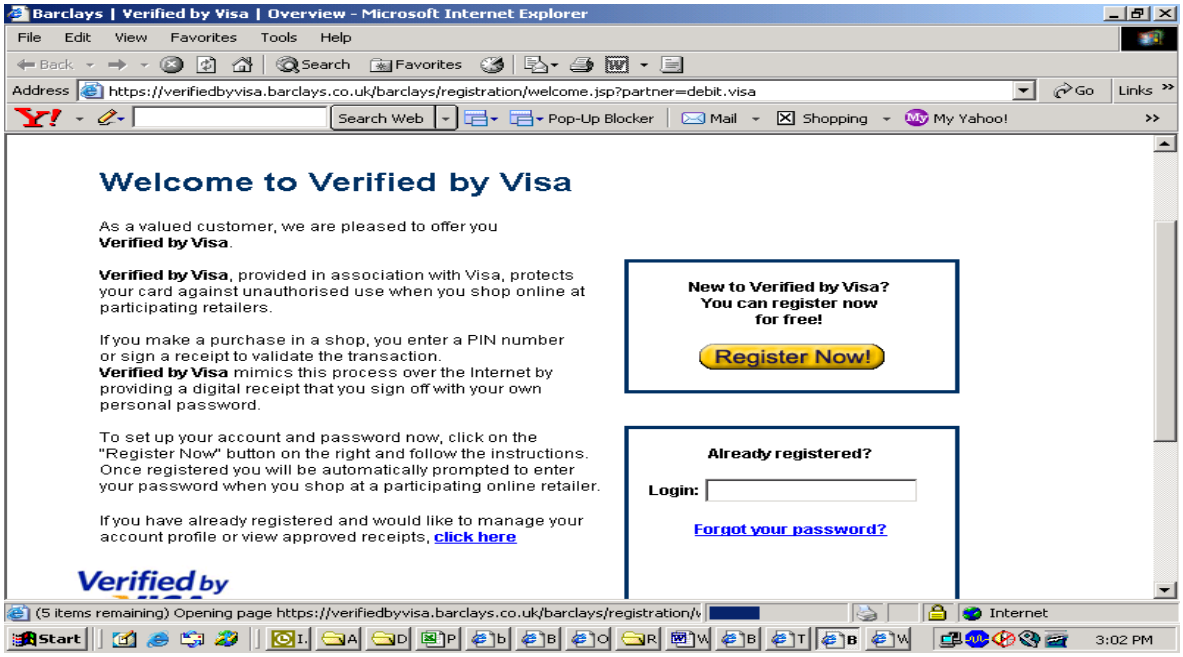
Barclays Banks log- in process to online internet banking has the following authentication grid as part of the bank's fight against online crime. The login process has multiple steps. The steps are as follows:

- Bank issues each customer with a unique membership number.
- Bank asks for customer surname as a piece of personal information a fraudster would not know in relation to a customer's membership number.
- A five digit passcode.
- Bank asks for 2 random letters from customer's memorable word. These letters are taken at random so that if someone is tracking customers keyboard's actions through a virus on computer, the letters will be different next time. The customer can change this memorable word online.



4.8.4 Online shopping verified by VISA.

Barclays bank in association with VISA has further tightened the security for online shopping. The customer is asked to register with VISA, thereafter every time if customer makes a purchase online, VISA asks the PIN for authentication.

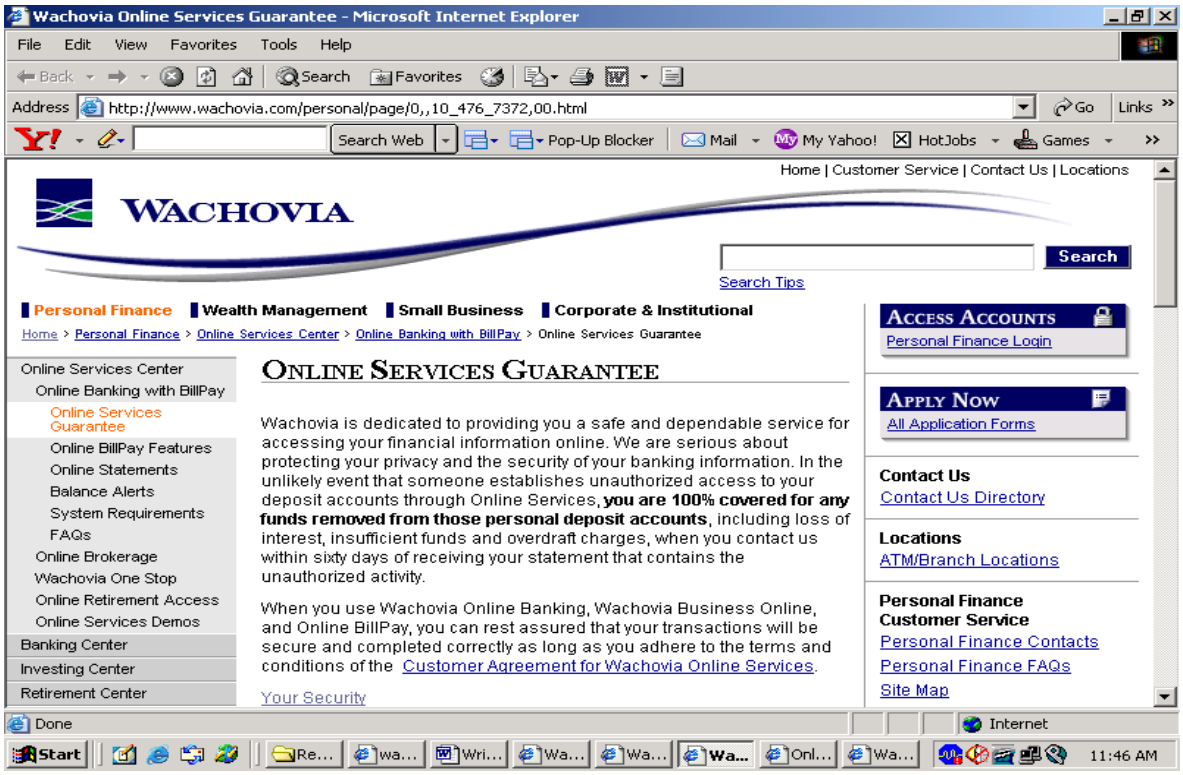


4.9 Wachovia Bank

Wachovia Bank the no. 36[9] bank in the world in terms of asset size, provide online service guarantee to prevent online fraud and phishing.

4.9.1 Online service guarantee.

Wachovia Bank provides guarantee to refund money to customers in the event of any unauthorized access to the customers accounts. The condition is that the customers have to be careful and report within sixty days of receiving the statement.



4.10 National Australia Bank.

National Australia Bank the no. 50[10] bank in the world in terms of asset size, has taken the following steps to prevent online fraud and phishing.

1) Two Factor authentication (SMS Payment Security)

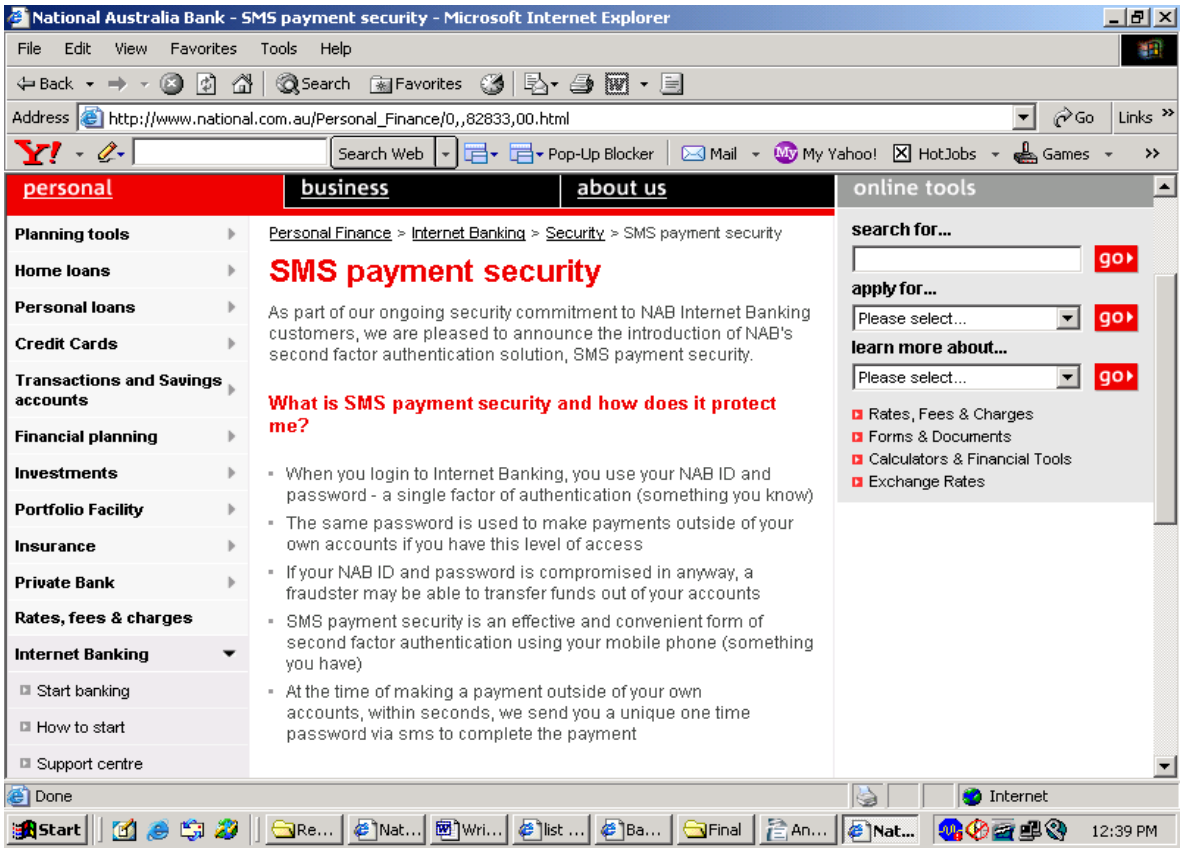
4.10.1 Two Factor authentication.

[9] As per published report in bankersalmanac.com website

[10] As per published report in bankersalmanac.com website

National Australian Bank (NAB) as part of its login process has implemented the second factor authentication i.e. SMS payment security. SMS payment security is an effective and convenient form of second factor authentication using the customer mobile. The authentication process is as follows

At the time, the customer is making a payment to a third party, within seconds, the customer receives a unique one time password via sms to complete the payment.



4.11 Royal Bank of Canada.

Royal Bank of Canada the no. 43[11] bank in the world in terms of asset size, has taken the following steps to prevent online fraud and phishing:

1) Two Factor authentication.
2) 100% reimbursement for unauthorized online banking transaction.

[11] As per published report in bankersalmanac.com website

4.11.1 Two Factor authentication.

The Royal Bank of Canada (RBC) as part of its login process has implemented the second factor authentication. To ensure the integrity of the systems and the safety of their customer information, RBC Online Banking uses several layers of robust security mechanism, technologies and processes. Sign-In Protection is the second level of authorisation that RBC has implemented as part of its fight against phishing and identity theft.

Like a second lock on door, Sign-In Protection adds an extra barrier between customer online accounts and any unauthorized users. The feature works when a customer signs in to online banking from any location i.e. using a publicly available computer - such as in a library or airport - or be signing in from home.

The system uses a combination of advanced safeguarding techniques to confirm identity. The customer will be asked to create three unique personal verification questions - answers to which only customers would know - such as the year and model of his first car or his favourites vacation spot.

Sign-In Protection will then prevent access to Online Banking information from any computer it doesn't recognize unless the correct answer to a personal verification question is provided.

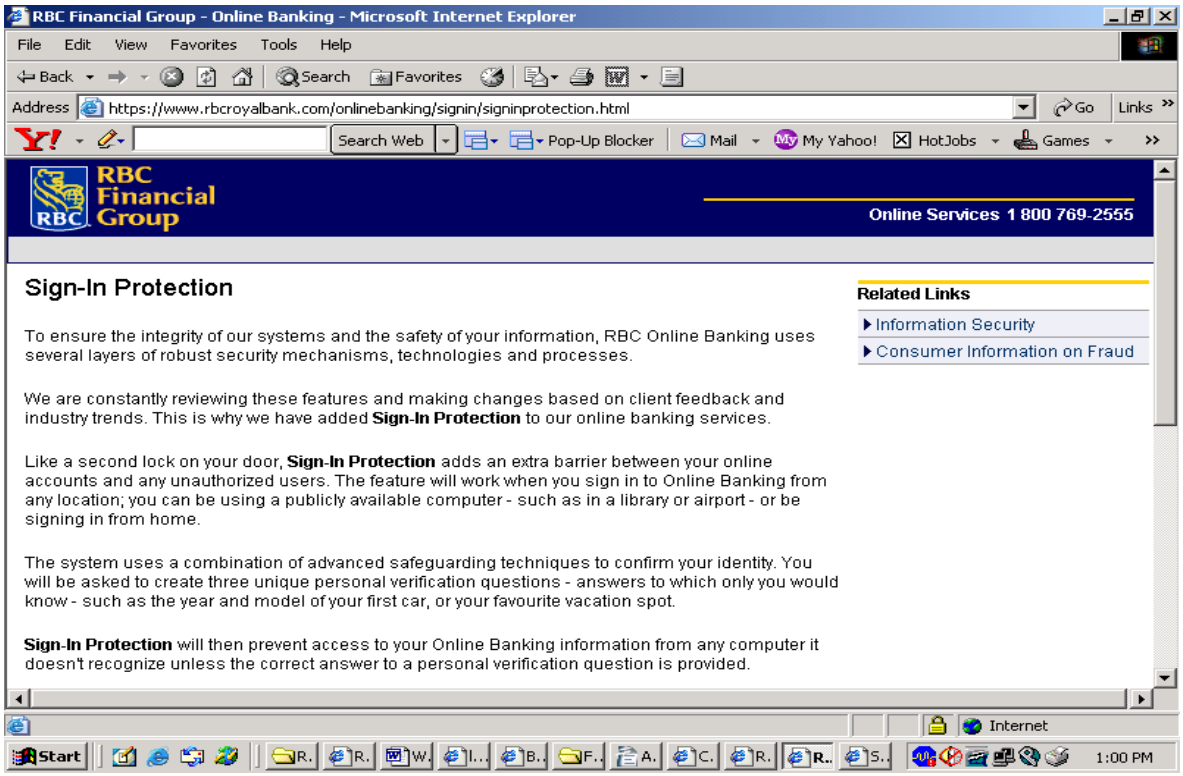
Step by step description of how Sign-In Protection works:

Step 1 – The customer enters the card number and password.

Step 2 - The customer click Sign In.

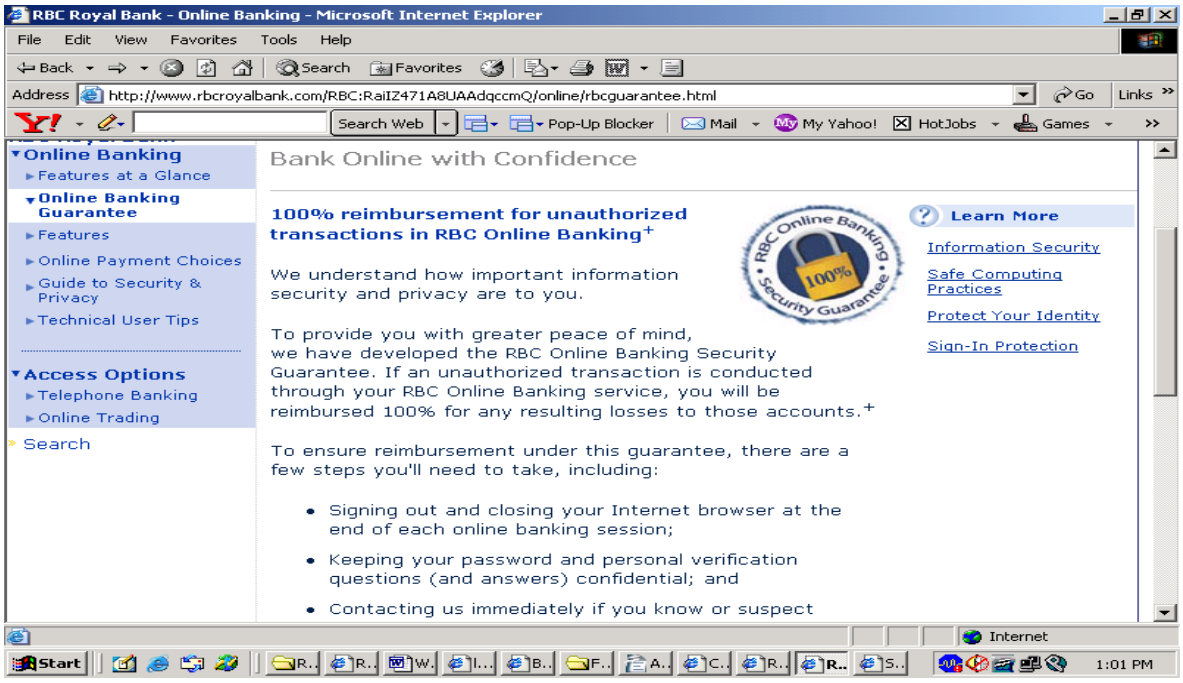
Step 3 - If Bank recognizes the computer, the bank will display the home page and the customer can safely begin his online banking session.

Step 4 - If Bank don't recognize the customer computer, Bank will ask one of the personal verification questions the answer of which is known only to the customer. Once correctly answered, the Bank will display the home page and the customer can safely begin his online banking session.



4.11.2 100% reimbursement for unauthorized online banking transaction.

Royal Bank of Canada provides a guarantee to refund money to the customer in the event of any unauthorized access to the customer accounts subject to certain conditions.

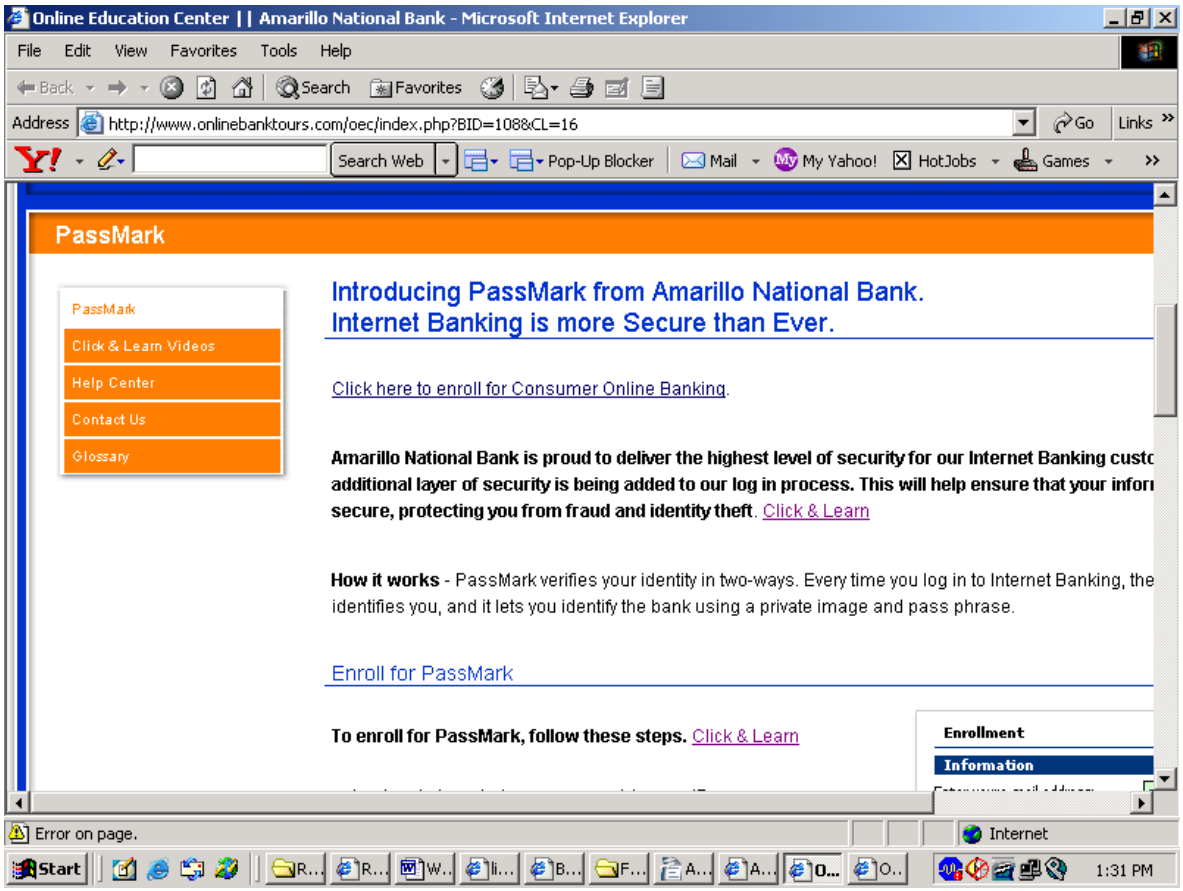


4.12 Amarillo National Bank.

Amarillo National Bank is based in the US. The Bank is a community based bank and is 110 years old. The Amarillo National Bank has taken the following steps to prevent online fraud and phishing.

1) Two Factor authentication

4.12.1 Two Factor authentication – PASSMARK.



Amarillo National Bank has added an additional layer of security to the log in process i.e. PassMark. This process will help ensure that the customer information is secure, protecting from fraud and identity theft.

PassMark verifies the customer identity in two-ways. Every time the customer logs in to internet banking, the bank identifies the customer, and it lets the customer identify the bank using a private image and pass phrase.

The steps are:

1. Log in by entering current Access ID.
2. Enter current password.

3. Complete the enrollment form.

    - Provide a current e-mail address (if needed).
    - Enter a phrase for the randomly selected authentication image.
    - Provide answers for 3 challenge questions.
    - Select whether the customer logs in with his personal computer or a public computer. Only register personal computers that the customer frequently uses and are not available for public use.
    - Complete the registration

The next time the customer logs in, PassMark will recognize the customer and display the private images and pass phrase.

The advantages are:

- The customer knows that the website is a genuine website of the Bank
- Even if the first level of password is compromised the fraudster will not know the answer for challenge question, which will be asked if the customer logs in through some unregistered computer.

4.13 Nantucket Bank.

Nantucket Bank is based in the US. The Nantucket Bank has taken the following steps to prevent online fraud and phishing.

1) Two Factor authentication.

4.13.1 Two Factor authentication – OnGuard.

The OnGuard Authentication - Enhanced Security for online banking is an effort to protect financial information and prevent identity theft. The new security feature and with the use of a more complex password for online banking helps preventing frauds and unauthorized usage of online banking. OnGuard provides strong authentication to protect the online account from unauthorized access.

In addition to the OnGuard system, a more complex password will be required - one that has a minimum of six characters including a combination of letters and numbers and contains at least one capital letter.

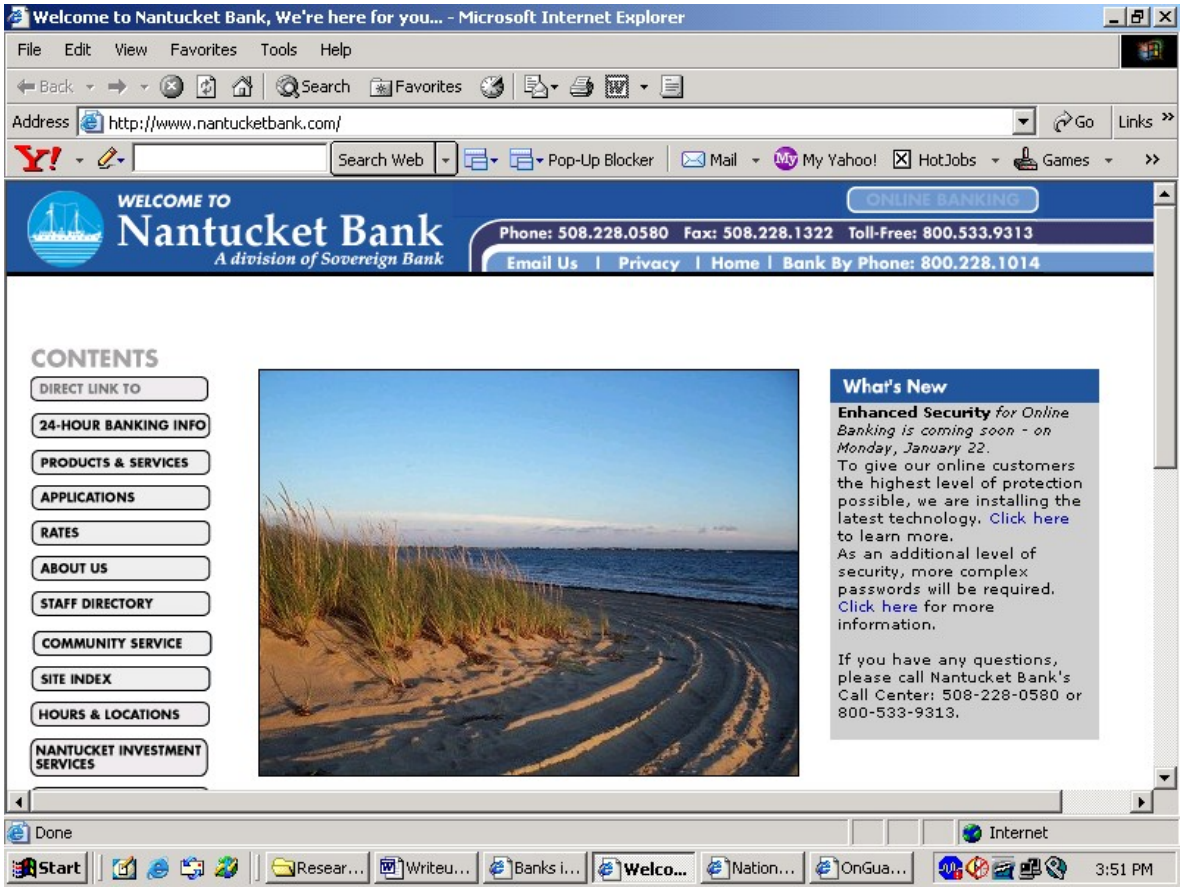
After initial logon, the customer will be asked to pick and answer several personal questions. During next few logons after having answered the personal

questions, this new high-tech system will recognize whether the customer continue to use the same computer and will not ask questions for further logins.

On Guard will compare over 15 different access characteristics to authenticate the customer access.

After OnGuard has enough access history, it will determine if the computer that is used to logon is different from the computer have been used in the past. If it is different, as well as at certain intervals, the customer will be asked to verify the identity by answering one of the selected questions.

Incorrect answers, the same as an incorrect logon ID and password, will prevent from accessing the account.



4.14 The countermeasure adopted by various Banks,summarized as follows:

	Countermeasure							
Bank /Companies	Anti-Phishing Toolbar	Security Question as a part of Log in authentication	Registration of Computer for doing online Transaction	Image Based authentication of website	SMS Based authentication	Anti – Virus Software (Free / Discount)	100 % refund due to online fraud	Online Shopping authentication
Bank of America	✓	✓	✓	✓			✓	
US Bank							✓	
Well Fargo Bank							✓	
Nat West Bank						✓		
Ebay & PayPal	✓							
Lyods TSB Bank						✓	✓	
Barclays Bank		✓			✓	✓	✓	✓
Wachovia Bank							✓	
National Australia Bank					✓			
Royal Bank of Canada		✓	✓				✓	
Amarillo National Bank		✓	✓	✓				
Nantucket Bank		✓	✓	✓				
Various other US Based banks								
Republic Bank		✓	✓	✓				
Lajolla Bank								✓
Central Bank			✓					✓
Bank United		✓	✓	✓				
Bank First		✓	✓	✓				

	Countermeasure							
Bank /Companies	Anti-Phishing Toolbar	Security Question as a part of Log in authentication	Registration of Computer for doing online Transaction	Image Based authentication of website	SMS Based authentication	Anti – Virus Software (Free / Discount)	100 % refund due to online fraud	Online Shopping authentication
Citizen Bank		✓	✓	✓				
Crown Bank		✓	✓	✓				
Gulf Coast Bank		✓	✓	✓				
Salem Five Bank		✓	✓	✓				
North Valley Bank		✓	✓	✓				
Peoples Bank							✓	
Capital One Bank							✓	
AM South Bank							✓	
Patel Credit union							✓	
Huntington Bank							✓	

As per Anti-Phishing group, phishing attacks are predominant in the US. The numbers of spoofed websites are hosted more in the US.

5. Conclusion.

Phishing attacks are a major threat to e-commerce and e-banking applications. The fraudsters are making huge gains by stealing financial data from users. There is a need for adoption of countermeasure steps by the Banks and individual customers for fighting phishing attacks. No single technology will completely stop phishing. However, a combination of customer-technology-organisation, proper application of currently available technology, and improvement in security technology has the potential to drastically reduce the hazards of phishing and the losses suffered from it.

6.0 References.

Anti -Phishing Working Group (www.antiphishing.org)
Report Title – Online Identity Theft: Phishing Technology, Choke points and Countermeasures available in website
Report Title – Phishing attacks and countermeasures - by Anil Sagar - CERT-In – Indian Computer Emergency Response Team
Report Title - Turning Identity Theft into A Business opportunity By Empowering Your Customers
Various Banks websites as listed in Table of contents

Disclaimers : The views mentioned are the personal views. Any reference should be at your own risk. The author is not any way responsible for any action taken based on the content of the article.