



Phishing Scams:

Understanding the latest trends

Trent Youl

June 2004

A White Paper presented by FraudWatch International, the Internet's high profile Fraud Prevention Web Site.



1. Introduction

Phishing has become the fastest growing scam on the Internet. Phishing occurs when fraudsters attempt to trick consumers into revealing personal information, such as financial account details, user login ID's & passwords and personal identification details. Deception tends to be the most used method, although Trojans and spyware are also used to capture this information.

FraudWatch International monitors phishing scams and has seen a huge increase in the number of phishing email scams reported to us. April saw an increase in excess of 250% compared to March, whilst May saw a further 215% increase compared to April.

Phishing scams are initiated with a fraudulent email, purporting to be from an official organization, such as a Financial Institution, Internet Service Provider or a well-known Internet Payment Processing Company. These emails are a malicious form of unsolicited bulk email commonly known as SPAM. The emails are supported by a fraudulent web site, impersonating the legitimate web site of the company they claim to be.

Images and styles on legitimate web sites can be easily copied to portray a fraudulent web site as genuine. Emails are constructed utilizing these images to create an apparent genuine email from the desired company. The emails request the recipient to divulge personal information. Reasons given include software upgrades, fraudulent activity and incorrect or unverified current information. These emails are designed to persuade the user to click on a link within the email to provide this information. The emails appear to be legitimate, and most sound professional, providing valid reasons why the recipient must provide their personal information. It is normal for the emails to provide a sense of urgency, and warn the user that if they don't follow instructions, they will lose access to their account through suspension or termination.

To pass the email as genuine, the fraudsters utilize various methods, including sender address forging or disguising the hyperlinked address of a link within the email. Once at the website, the user is further deceived by methods including URL spoofing, hiding the address bar, creation of a false address bar and genuine looking content.

After providing personal information, the user is further deceived by various methods including the display of confirmation web pages or error messages (if they have attempted to log in to their account), coupled with redirection to the genuine web site. The user is often unaware they have provided their personal information to fraudsters.

Fraudsters store and utilize personal information they receive by hijacking user accounts, fraudulently using credit cards, duplicating ATM cards, creation of counterfeit checks using account information, and possibly the most frightening use; duplicating a victim's identity in an Identity Theft scheme. This information allows the fraudsters to obtain credit using the victim's personal information.

The recent targets of phishing scams have been large financial institutions, Internet payment processing company Paypal and online auction giant eBay. Whilst this trend will continue, we expect phishing scams to move towards smaller financial institutions and other companies, such as telecommunications and utility companies, who accept payment for services via the Internet.

Proposed changes to the structure of email technology to assist in the reduction of SPAM and associated phishing emails are long-term solutions. These changes will take time to be delivered to the wider Internet community. Phishing email scams require a more urgent short-term solution.

In our opinion consumer education is the key to the reduction of recipients becoming victims of phishing email scams. Consumers need to be educated on the methods used to defraud them, and of systems they can put in place to protect themselves from becoming a target.

This white paper provides an in depth discovery of the current trends used to deceive consumers and looks at prevention measures both corporations and consumers can utilize, in an attempt to minimize the impact of phishing scams.

2. Statistics

Statistics of phishing attacks reported in May 2004 to FraudWatch International show an increase of 215% compared to attacks reported during April 2004.

Exact statistics of the number of phishing attacks are difficult to establish. Organizations such as FraudWatch International rely on the reporting of these attacks from consumers who receive the emails, and the companies who are targeted. This method is by no means scientific and the compilation of complete and accurate statistics is a challenging, if not impossible task.

There is a general consensus that these attacks have dramatically increased since their emergence mid 2003. The Anti-Phishing Working Group (APWG) reported a 180% increase in attacks from March to April 2004*, whilst FraudWatch International's figures suggested a significant increase in excess of 250% for the same period. These statistics could also be an indication of increased consumer awareness and reporting of the attacks.

Financial sector companies are the main targets of phishing attacks, receiving between 50 - 75% of attacks, depending on the source of reports.

Whilst no substantial reliance can be placed on these statistics, one safe conclusion can be drawn: Phishing attacks are posing a serious threat to the stability of consumer trust in the Internet, particularly with providing personal or financial information through activities such as Internet Banking and e-commerce.

*Source: Anti-Phishing Working Group Phishing Attack Trends Report April 2004. www.antiphishing.org

3. Phishing Methods Used

There are a number of methods used by fraudsters in phishing scams:

- Deception Methods
- Malicious Software (Trojans)
- Spyware

1. Deception Methods

Initial Phishing Email:

The initial phishing email is designed to entice the recipient to open the email and click on the link provided. The fraudsters use multiple methods to do this, including enticing subject lines, forging the address of the sender, using genuine looking images and text and disguising the links within the email.

Subject Line

Phishing emails tend to have subject lines that appear to be genuinely related to who the email is from, in an attempt to entice the user to open the email. For example, subject lines such as "Important notice for all Internet Banking Users". It is also common for subject lines to carry numerals or other letters to replace characters, in an attempt to bypass SPAM filters, such as capital "I" replacing "l". Some phishing emails will deliberately misspell key words to bypass SPAM filters, which most people would not recognize when quickly glancing at the subject line.

Forged Senders Address

The forging of the senders address is an easy deception method. There is no guarantee that the address listed as the senders address is genuine. Phishing scam emails will normally have a forged senders address appearing as though the email has come from the company it is claiming to be.

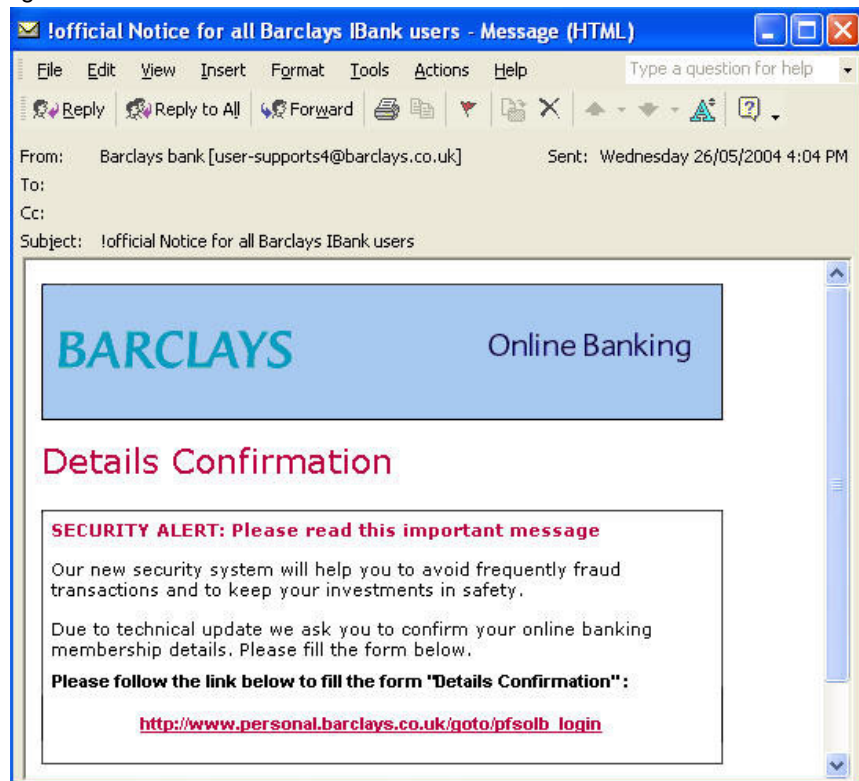


Figure 1: Barclays Bank phishing email. Note deception techniques: subject line, forged senders address, genuine looking content and forged links.

Genuine Looking Content

Phishing emails normally utilize copied images and text styles used on the legitimate web site to portray their email as genuine. Many consumers are fooled into thinking an email is genuine simply because it had the bank's logo within the email. Some phishing emails also have genuine links to the company's privacy policy and other pages on the legitimate web site. Trusts and authentication marks are also duplicated to build the user's confidence in the authentication of the email.

Disguised Links

Links within an email are deliberately disguised in another attempt to deceive the recipient. HTML emails may display a genuine URL but when clicked on the hyperlink will take the user to a different web site. For example: a link displayed as "http://www.genuine-site.com" may actually take the user to "http://www.fraud-site.com"

In text only emails, a long URL would be presented with an "@" before the actual web site. For example, a link may be displayed as

"http://www.genuine-site.com-Verify83kcmdj30dk>Secure32902ds;lkjasdfkljad@fraud-site.com"

This would take the user to http://www.fraud-site.com, as this is after the @ symbol. The link may look valid because it begins with the genuine site URL, and contains genuine looking words within the link.

These methods are used by the more complex phishing emails. Some amateur phishing emails may contain poor spelling & grammar, no images and may not even attempt to disguise the URL.

Fraudulent Web Sites:

The fraudulent web site that supports the phishing email is designed to mirror the legitimate web site it is purporting to be. The fraudsters use multiple methods to do this, including using genuine looking images and text, disguising the URL in the address bar or removing the address bar altogether. The purpose of the web site is to trick consumers into thinking they are at the company's genuine web site, and giving their personal information to the trusted company they think they are dealing with.

Genuine Looking Content

Phishing web sites utilize copied images, text and in some cases simply mirror the legitimate web site. This will contain the normal links on the web site such as contact us, privacy, products, services etc. The user recognizes the website content from the genuine site and are unaware they are not on the genuine web site.

Similar URL to the genuine URL

Some phishing web sites have registered a domain name similar to that of the organization they are appearing to be from. For example, one phishing scam we received targeting Barclays Bank used the domain name "http://www.barclayze.co.uk". Other examples include using a sub-domain such as "http://www.barclays.validation.co.uk", where the actual domain is "validation.co.uk" which is not related to Barclays Bank.

Incorrect URL

Some phishing scam web sites do not even attempt to deceive users with their URL, and hope that the user does not notice. Some simply use I.P Addresses displayed as numbers in the users address bar.

URL Spoofing of Address Bar (Fake Address Bar)

This form of URL spoofing involves the removal of the address bar combined with the use of scripts to build a fake address bar using images and text. The link in the phishing email opens a new browser window, which closes and re-opens without the address bar, and in some cases the status bar. The new window uses HTML, HTA and JavaScript commands to construct a false address bar in place of the original. (See figure 2 below)

As this method utilizes scripts, it is only possible to stop this form of deception by disabling active x and JavaScript in browser settings. As most web pages utilize these normal tools, this is impractical.



Figure 2: Fake Address Bar displayed. Notice the change in colour on the right? You can also observe if you click on the drop down arrow on the address bar, the history is empty.



Figure 3: A closer look. Right click on a toolbar, tick address bar. This shows the correct address bar with the correct URL.

Hovering text box over Address Bar

This form of URL spoofing involves the placement of a text object with a white background over the URL in the address bar. The text object contains the fake URL, which covers the genuine URL.

As this method utilizes scripts, it is only possible to stop this form of deception by disabling Active X and JavaScript in browser settings. As most web pages utilize these normal tools, this is impractical.

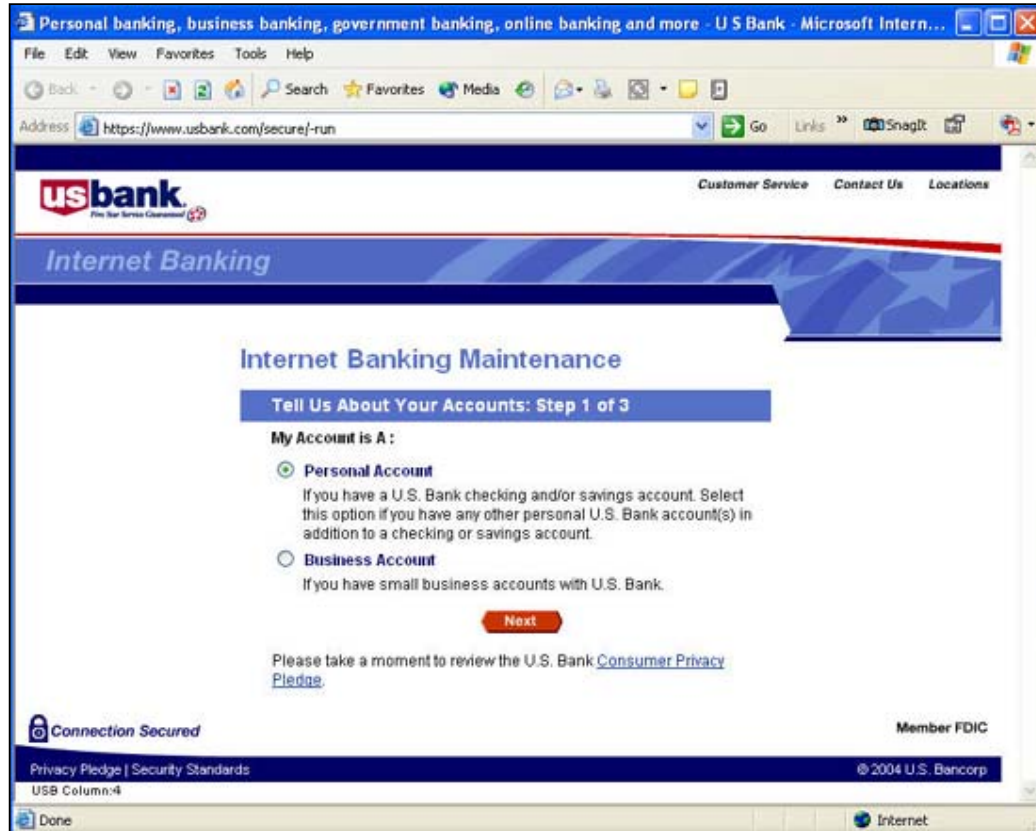


Figure 4: Fake Address Bar displayed using a hovering text box. Virtually impossible to pick when glancing at the address bar.

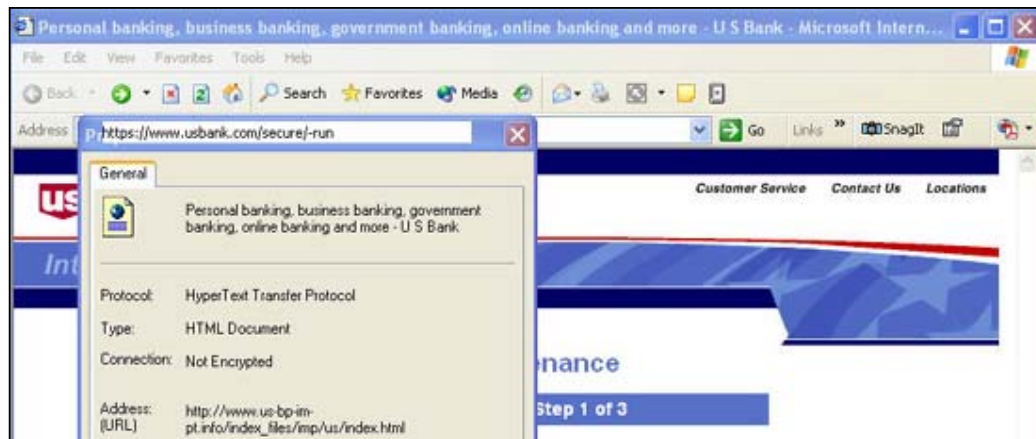


Figure 5: A closer look. Select Properties from the File menu. The properties box shows us the correct URL, whilst also highlighting the white text box hovering over the address bar.

Two Pages Displayed – Pop Up Windows

This form of deception involves the use of script to open a genuine webpage in the background while a bare pop up window (without address bar, tool bars, status bar and scrollbars) is opened in the foreground to display the fake webpage, in an attempt to mislead the user to think it is directly associated to the genuine page. (See figure 6 below)

As this method utilizes scripts, it is only possible to stop this form of deception by disabling Active X and JavaScript in browser settings. As most web pages utilize these normal tools, this is impractical.

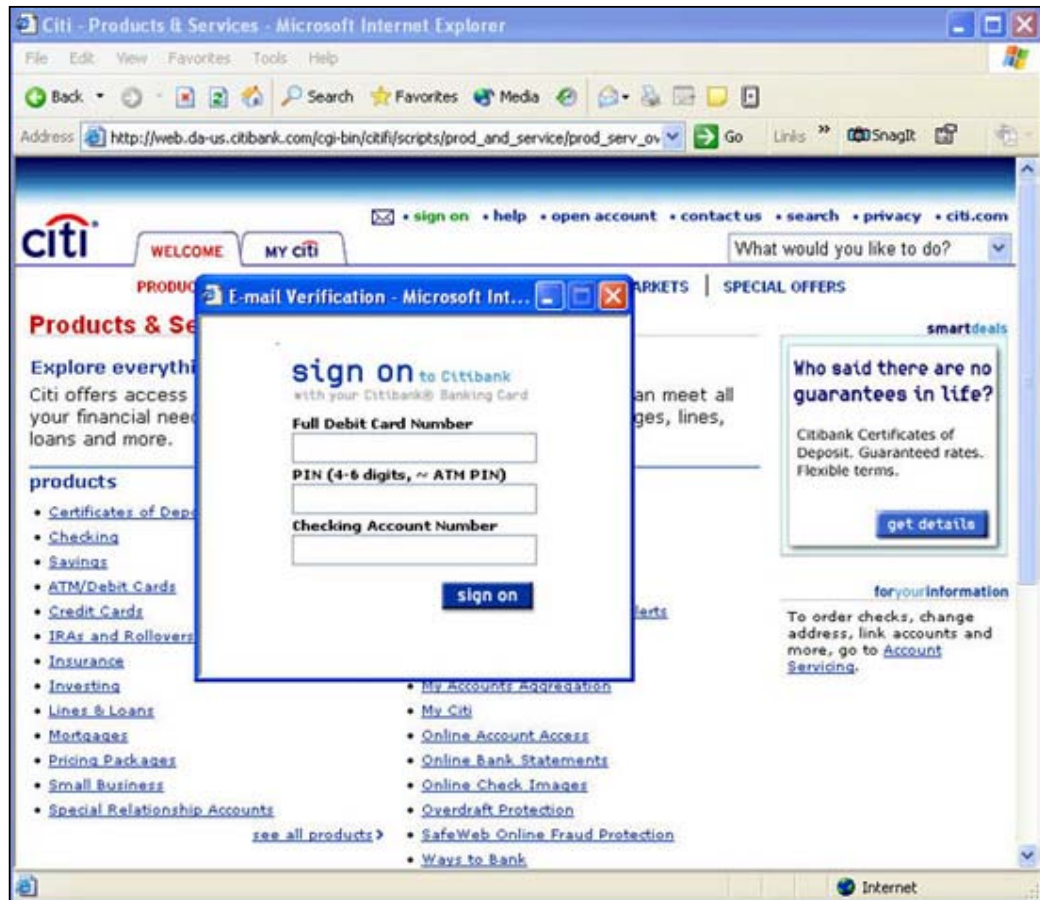


Figure 6: Genuine Citibank webpage is displayed in the background, while the fake webpage is displayed in a pop up window in the foreground.

2. Malicious Software (Trojans)

Trojan and worm viruses are sent to the user as an email attachment, purporting to be for some type of purpose, such as greetings, important files or other type of SPAM email. The attachment is a program that exploits vulnerabilities in Internet Browsing software to force a download from another computer on the Internet. This file downloads other files and codes, which eventually installs a fully functional Trojan virus.

The Trojan is designed to harvest, or search for personal banking information and passwords, which many people keep on their computer. This information is then sent to a remote computer on the Internet.

Other worms have been known to hijack the user's HOST file, which causes an automatic redirection to a fake phishing web site when the user types in a specific URL (normally for a specific financial institution) into the address bar of their Internet browser.

3. Spyware

Spyware, such as keyboard loggers, capture information entered at legitimate web sites, such as Internet banking sites. This type of spyware can be planted on a user's computer using a previous worm or Trojan infection. Any information the spyware captures is sent to a predetermined computer on the Internet.

A recent phishing scam used the link in the email to direct the users browsers to a site to first download keyboard logging spyware before redirecting the user to the genuine Internet banking web site. This spyware captured the login information entered, and sent this information to the fraudsters via a remote computer on the Internet.

4. What happens to the personal information when collected?

There are a number of ways in which personal information collected is used by the fraudsters:

- Hijacking user accounts
- Fraudulent use of credit cards
- ATM card duplication
- Identity Theft

1. Hijacking user accounts

If the victim provided bank account information, the fraudsters are likely to hijack the victim's bank account; access passwords can be changed, locking the victim out of their account. The fraudsters may empty the victim's bank account by electronically transferring funds to a temporary account they have fraudulently set up using someone else's personal information. The cash is then withdrawn before the victim is aware what has happened.

The fraudsters may also create, write and cash fraudulent counterfeit checks on the victim's account. In this way, the victim has no idea they have been defrauded until they notice cash has left their account.

The fraudsters may also store the account information, waiting for a time when there is the desired amount of money in the account. The victim has no idea, until it's too late.

2. Fraudulent use of credit cards

If the victim provided credit card details, it is likely their card details will be used to make unauthorized fraudulent purchases.

The credit card information may also be sold to organized fraud rings, weeks or months down the track. The victim is unaware their credit card information is in the hands of fraudsters until they begin to see unauthorized charges on their statement, or they try to use their card and it has been maxed out.

3. ATM card duplication

There has been a trend of phishing scams that require the user to provide their ATM card number, expiry date and ATM pin. This allows the fraudsters to create duplicate ATM cards, linked to the victim's debit card account. The victim's account may be cleared out through ATM withdrawals.

4. Identity Theft

Identity Theft is the use of someone's personal information without their knowledge to apply for credit cards, make unauthorized purchases, gain access to bank accounts and apply for credit. Often, credit is obtained using the victim's name and personal information, who is then left to explain the credit and clear their name long after the fraudsters has disappeared.

Identity Theft is reported to be the world's fastest growing crime. In the past, fraudsters would trowel through rubbish bins and letterboxes looking for documents with personal information. Now they simply ask the victims for the information, in the form of phishing scams.

Personal information is traded amongst identity thieves. Whilst the phisher's themselves may not use the personal information, it may be sold to identity thieves who will then use it to meet their needs. False credit can provide fraudsters with an anonymous way to survive and financially support illegal operations.

Incidence of Identity Theft in the U.S. has grown by more than 40% in 2003 compared to the previous year. The Federal Trade Commission estimates 4.7% of the U.S. population, or 10 Million people were victims of Identity Theft in 2002, with total losses of US\$53 billion. Of this US\$5 billion was lost by victims, the remaining losses were picked up by businesses, including financial institutions. [U.S. Federal Trade Commission – Consumer Sentinel Report 2003]

5. Prevention

Although complete prevention is virtually impossible, there are some logical precautionary measures that both consumers and corporations can take in an attempt to reduce the potential of being conned by phishing scams.

CONSUMERS

1. SPAM Filters

Effective SPAM filters can reduce the number of fraudulent and malicious emails consumers are exposed to. SPAM filters can be applied at the Internet Service Provider's email gateway, or as software on the user's computer. It is recommended that both filters be applied to all emails.

2. Anti-Virus Software

To protect against Trojan and worm attacks, anti-virus software can detect and delete virus files before they can attack a computer. It is important to keep all anti-virus software up to date with vendor updates.

3. Personal Firewall

Firewalls can monitor both incoming and outgoing Internet traffic from a computer. This can protect the computer from being hacked into, and a virus being planted, and can also block unauthorized programs from accessing the Internet, such as Trojans, worms and spyware.

4. Padlock & "https://"

When submitting sensitive financial and personal information on the Internet, look for the locked padlock on the Internet browser's status bar or the "https://" at the start of the URL in the address bar. Although there is no guarantee of the site's legitimacy or security if they are present, the absence of these indicates that the web site is definitely not secure.

5. Links in emails

Consumers should not click on hyperlinks within emails that are apparently from a legitimate company. Instead, directly type in the URL in the Internet browser address bar, or call the company on a contact number previously verified or known to be genuine.

6. Update Software

Always ensure operating and browser software is kept up to date using legitimate upgrades and patches issued by the software vendor. This can help protect against known security issues within some software.

7. Education

Internet Fraud methods are evolving at a rapid rate. Consumers need to be aware they are vulnerable as fraudsters are persuasive and convincing; many victims thought they were too smart to be scammed. Consumers should educate themselves on Internet Fraud, the trends and continual changes in fraudulent methods used. FraudWatch International offers consumer education as a free service to the Internet community.

8. Seek Advice

If unsure as to the legitimacy of an email, consumers should seek advice from the legitimate corporation using verified contact details. For other potentially fraudulent emails, consumers can seek advice from FraudWatch International by forwarding the email with their questions to scams@fraudwatchinternational.com. This is a free service to assist in the prevention of Internet Fraud.

CORPORATIONS:

1. Corporate Email Policies

Corporations should establish consistent corporate email policies and communicate them to their consumers. These could include the use of personalized emails to consumers, avoiding the use of forms and hyperlinks within emails, or utilizing other personalization techniques so the consumer recognizes the email is from the legitimate corporation, such as image identification specific for each consumer.

2. Personalize Emails to Consumers

Emails to consumers should always be personalized with their first and last name, and possibly other information that may not be easily gained by fraudsters. If the consumers is aware of what to look for, this could prove to be a simple method of making email communications with consumers more reliable.

3. Communication avenues for Consumers

Always provide an avenue to allow consumers to verify the legitimacy of any email received. This should be both a telephone number and an email address posted on the company's web site. Make it easy for consumers to verify emails.

4. Web Site Certificates

Web site certificates should be current to assure consumers of the web site's legitimacy.

5. Monitor the Internet for Potential Phishing Scams

Corporations should employ monitoring techniques that will identify a fraudulent phishing web site in a timely manner. There are some options that will monitor for unauthorized use of names, brand names and trademarks. We believe a faster and more valuable method of detecting phishing web sites is the monitoring of circulating phishing emails.

6. Rapid Response to Phishing Attacks

Corporations must ensure they are prepared for phishing attacks. Whilst a corporation may not have been a phishing target to date, chances are they may become a target in the future. Rapid Response Plans must be developed and tested. Much damage can be done to a corporation's brand and image if they are not sure what to do when targeted.

7. Support Consumer Education

Internet consumers need to be educated of the risks and potential pitfalls. Corporations must recognize the potential implications to their brand and reputation should they become the target of a phishing attack. Educating consumers before this can minimize the potential damage. Both current and potential consumers need to be educated. Corporations must realize the value and responsibility they have in educating consumers.

6. Future of Phishing Scams

The dramatic increase of phishing scams over the past 8 months is a concern for the Internet community as a whole. Phishing is providing a relatively easy method for fraudsters to operate anonymously. This increase highlights the fact that fraudsters are achieving adequate success.

Proposed changes to the Internet's structure of email technology to assist in the reduction of SPAM and associated phishing emails are long-term solutions. These changes will take some time to be delivered to the wider Internet community. Even when these systems are changed, it is likely that phishing scams will be changing at the same time.

Whilst the recent targets of phishing emails have been large financial institutions, we anticipate that phishing scams will move towards smaller financial institutions and other corporations that deal with financially sensitive data on the Internet. As more corporations transfer their billing and e-commerce activities to the Internet, we believe phishing scams will change their approach and become more specific with the targeting of email users.

We see no immediate reduction in the number of phishing scams circulating the Internet. With the number of new Internet users increasing daily it is highly probable that phishing scams will increase in their success rate, unless immediate action is taken.

FraudWatch International believes that the best tool against phishing scams is consumer education. Consumers need to be educated on the methods used to defraud them, and of systems they can put in place to protect themselves from becoming a victim.

Governments, law enforcement authorities, financial institutions, Internet Service Providers (ISP's), software manufacturers and all corporations wishing to do business on the Internet must address consumer education. A joint effort on behalf of these parties in educating consumers would see the overall success and subsequent costs of phishing scams reduce.

7. Conclusion

Phishing emails and web site attacks, have provided a faceless opportunity for fraudsters to reach millions of potential victims, with little cost outlay, in the hope of victims supplying their personal and financially sensitive information. This information is then used to hijack accounts and duplicate the victim's identity through the fastest growing crime in the world, Identity Theft.

It is apparent that fraudsters perpetrating phishing scams are becoming more technologically efficient, utilizing smarter deception methods to create and implement their phishing scams.

Whilst there is no quick fix solution to phishing scams, both consumers and corporations can take some precautionary action in an attempt to reduce their potential of being conned by phishing scams.

In our opinion consumer education is the key to the reduction of consumers becoming victims of phishing email scams. Education should be the focus and combined effort of governments, law enforcement authorities, financial institutions, Internet Service Providers (ISP's), software manufacturers and all corporations wishing to do business on the Internet.

FraudWatch International is committed to reducing the incidence of Internet Fraud and protecting consumers from Identity Theft where personal and credit information is collected by fraudulent and deceptive means. Consumer education is our number one priority. FraudWatch International offers a free service to educate and advise Internet consumers around the world.

About FraudWatch International

FraudWatch International is an Internet Fraud education, prevention and investigation web site managed by The Confidence Group Pty Ltd, a company based in Melbourne, Australia.

FraudWatch International was launched in June 2003 and has since had hundreds of thousands of visitors and has shut down countless scams. As our profile continues to grow within the global Internet community we continue to add value to consumers and corporations around the world.

Many consumers have been saved from financial loss by utilizing the information on our free educational web site, or asking us questions regarding potentially fraudulent emails and web sites.

FraudWatch International receives thousands of fraudulent emails each week, which are investigated by our Investigations Team. We request the web hosting company to immediately shut down any sites that proves to be fraudulent. This is an invaluable service to consumers and corporations, which are the targets of these scams. There is no method to calculate the exact losses we have prevented, but it would be safe to say we have saved both consumers and corporations hundreds of thousands of dollars through our efforts.

As we continue to grow, FraudWatch International is seeking to build relationships with the major cost bearers of Internet Fraud and strengthen relationships with Government and Law Enforcement agencies around the world.