International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:4, No:9, 2010

Efficacy of Anti-phishing Measures and Strategies - A research Analysis

Gundeep Singh Bindra

***Abstract*—**Statistics indicate that more than 1000 phishing attacks are launched every month. With 57 million people hit by the fraud so far in America alone, how do we combat phishing?This publication aims to discuss strategies in the war against Phishing. This study is an examination of the analysis and critique found in the ways adopted at various levels to counter the crescendo of phishing attacks and new techniques being adopted for the same. An analysis of the measures taken up by the varied popular Mail servers and popular browsers is done under this study. This work intends to increase the understanding and awareness of the internet user across the globe and even discusses plausible countermeasures at the users as well as the developers end. This conceptual paper will contribute to future research on similar topics.

***Keywords*—**Anti-phishing, countermeasures, effectiveness, fake pages, security analysis.

I. Introduction

IN the field of computer security, Phishing is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication [1].

Fundamental Steps of the Phishing Attack:-

1. In the first step, the phisher just downloads the web pages from the legitimate websites that he wishes to attack and then creates, through web coding, a webpage which resembles the original web page in look and feel.
2. Then once the web pages are ready the phisher works on the php script linked with the fake page, which in the background traps the user's sensitive details and redirects to a particular URL, mostly the original domain that the phisher tries to attack.
3. The files required by the phisher are to be uploaded at the web hosting site which can be either free or priced as per the phisher's choice based on case to case. In some cases , domains similar to the original one (which can be easily overlooked by the user) is purchased and phishing is carried out on that domain such as *maill.google.com* instead of *mail.google.com*.
4. Further, the phisher sends the link using his social engineering techniques through a very luring mode of communication (e-mail, telephone, instant messaging etc) and manages to convince the victim to go and visit the fake page and enter his secret information which gets trapped in the linked database under the control of the phisher.
5. Finally, the information is used by the phisher in a malicious way to carry out activities such as Identity Thefts.

Phishing is an immorally deceitful process in which phishers are always trying to use more sophisticated activities to circumvent detection and user suspicion.

To minimize the impact of phishing attacks we need to look at *protection* (What can we do to save our users from falling prey to phishers ?), *fast and accurate detection* (How do we detect when an phisher is building a fake website and communicating to users?) and *effective response measures* (What can we do to minimize the impact once a successful phish has been launched?) The objective of this study is to examine the various plausible ways illustrating the countermeasures for the same.

II. Statistical Data

Statistics indicate that there were at least 126,697 phishing attacks in 2H2009. This is more than double the 55,698 attacks we recorded in 1H2009 on 28,775 unique domain names and 2,031 unique IP addresses [2].

TABLE I
Basic Statistics

	2H2009	1H2009	2H2008	1H2008
Phishing Domain Names	28775	30131	30454	26678
Attacks	126697	55698	56959	47324
TLDs Used	173	171	170	155
IP-Based Phish (Unique IPs)	2031	3563	2809	3389
Maliciously registered domains	6372	4382	5591	-
IDN Domains	12	13	10	52

provided by Anti-Phishing Working Group (APWG)

As is evident below in Fig. 1, the number of unique phishing reports submitted to APWG in the Q4, 2009 saw a substantial drop off after reaching an all time high of 40,621 in August, dropping to 28,897 reports in December, a decline of nearly 29 percent from that record high [3]. Still we cannot sit back and relax and leave the issue . This publication aims

G. S. Bindra is with the Department of Computer Science, SRM University, NCR Campus, New Delhi 201204 India (phone: +91-9896419601, +91-8010067705 ; fax: +91-1662-281005 ; website: http://gundeepbindra.com e-mail: mailbox@gundeepbindra.com;).

to discuss strategies in the war against Phishing and give it a further shot in the arm.

Fig. 1 Phishing Email Reports and Phishing Site Trends– 4th Quarter 2009 [3]

III. Objectives

1. The immediate objective of this research review paper is to carefully examine the ways in which phishing can be combated. Future work and advanced methodologies can be developed for the same.
2. One more supplementary objective is to draw comparisons between various popular Mail servers and browsers along with identifying the critical immediate measures to be researched and adopted.

IV. Measures

There can be measures taken up at various levels. The mail service could provide an anti-phishing measure or it can even be at the browser level. Each browser does has its own anti-phishing strategies or policies.

The measures taken up by various mail service providers and varied popular browsers are detailed below under following heads.

V. Measures At The Mail Server End

A. Yahoo! Mail – by Yahoo! Inc.

1) Yahoo Sign-In Seal

Yahoo recently launched Sign-In Seal [4] in an attempt to thwart phishing attacks. The concept is similar to the SiteKey used by Bank of America some time back. A Sign-In Seal is a secret message or an image selected by the user that Yahoo displays on the user's computer every time the user visits Yahoo from the same machine (i.e it tracks the IP address of the machine and provides the same interface from the same IP).

The Sign-In-Seal enables the user to make sure that they are on a genuine Yahoo site and this makes the attack of the phisher rather impossible as he is unaware of the exact seal on that system. If at all the attacker gets a physical access to the system, the story becomes the same and comes back to the original problem as the phisher can design the same interface to trap the user.

Steps to create a sign-in seal so that you know you are signing in on a genuine Yahoo! Website [5].

1. On any Yahoo! sign-in page, click “Create your sign-in seal” at the top of the "Sign in to Yahoo!" box. (a snapshot is shown below).
2. Click Create a text seal or Upload an image.
3. Type your secret message or select an image.
4. Click Save This Seal. This seal created will appear on the yahoo sign-in page, every time you open it from the same computer.

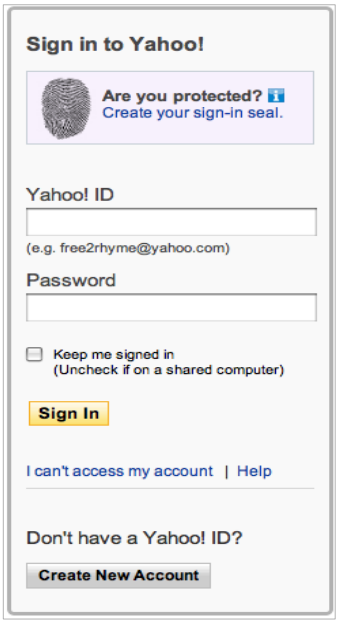

Fig. 2 Yahoo! Sign-in Seal [6]

Yahoo! Sign-in Seal is only associated with a browser/computer and not with a user’s account. Setup does not require any account information – even when setting up on different computers. Additionally, the Sign-in Seal is based on a personal picture instead of stock photographs, which is intended to increase affinity for the image [7].

2) Domain-Keys

Domain-Keys [8] try to crosscheck e-mail messages to verify their origin. Domain-Keys attach encrypted digital tags to each e-mail. Each e-mail is then compared with a publicly-available database of legitimate addresses.

3) Certified Email

Certified Email [9] is a feature which adds a layer of

protection to your Yahoo! by differentiating between the legitimate and the fake senders by seeing the Certified Email icon in your mailbox next to the sender's ID.

4) Phishing Tips

1. Don't believe every warning you read.
2. Do NOT click any button in these pop-ups.
3. There is no Yahoo! Lottery.

B. Gmail – by Google.

1) Report Spam

Gmail has also provided a prominent "Report Spam" button to its users. Any messages reported as spam get sent to a separate folder and Google's anti-spam software is notified.

2) Hypertext Links

The anti-phishing security feature disables “hypertext links” inside e-mails. Georges Harik, director of Googlettes said "We want to make it the best e-mail service in every single dimension, so you have absolutely no reason to use any other" [10]. Still I feel Gmail has a long way to go to develop great measures to protect phishing attacks in reality.

3) Warning Message

In one of its ventures, Gmail has impressed me with one of its initiatives in which it actually displayed a warning message (shown in Fig. 3) in a red box making authenticity of the sender very explicit.

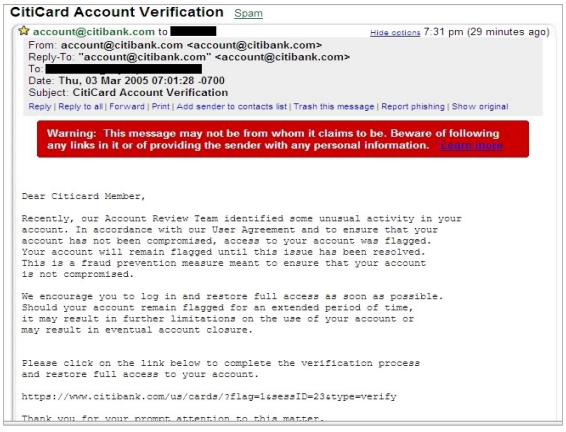

Fig. 3 Gmail's attempt to block phishing mail [11]

4) Gmail Labs: Super-trustworthy

When we do talk about Gmail labs, there is a very interesting feature "Authentication icon for verified senders" that adds an extra bit of reassurance. A very little key icon is placed next to the sender if the sender is "Super-trustworthy" [13]. The Official Gmail Blog also suggests you to choose a smart password [14].

5) Domain-Keys

Domain-Keys being Google's innovation, are used to check the source of the e-mail.

However, Gmail can still efficiently use their Gmail Lab features like Gmail themes [12] (already existent) to provide an interface before the actual Gmail login page based on the IP address or hardware address of the machine. This will give Gmail a good equivalent to the Yahoo's Sign-in-Seal we did talk about earlier.

C. Hotmail – by Microsoft Corporation

1) SmartScreen® Technology

To help reduce the consequences of junk e-mail, Windows Live Hotmail includes junk e-mail protection using patented SmartScreen® technology [15] which screens e-mails to identify and separate junk e-mails from legitimate ones. Machine learning refers to the probability-based algorithms that are used to distinguish between the different characteristics of legitimate and junk e-mail.

2) Hotmail Filters

Windows Live Hotmail also gives each user the ability to set filter levels to further improve the delivery of e-mails to their account. Users can easily add a sender or domain name to the Safe Senders and Domains List so that the e-mail from that sender or domain is never treated as junk regardless of the content of the message [16].

3) Anti-Phishing Technology

Microsoft is focusing its anti-phishing technology efforts on two fronts [17]: first by helping to prevent phishing e-mail messages from reaching our customers and secondly helping to eliminate the possibility of customers being deceived by spoofed e-mails and websites.

4) Sender ID

Spoofing is a way of replicating or imitating a legitimate e-mail address to give a fraudulent e-mail the appearance of legitimacy. Sender ID [18], an e-mail industry initiative championed by Microsoft and other industry leaders, is designed to verify that the sender’s actual location is the same as the one claimed in the e-mail address.

D. Rediffmail – by Rediff.com

Besides the the normal steps such as user awareness towards phishing, there is a very innovative tactic to deal with

the phishers. Rediffmail doesn't provide any login page. Instead it is contacted when clicked on the “Sign In” button at the rediff homepage resulting in a pop-up dialogue box asking the users then to enter their log-in credentials.

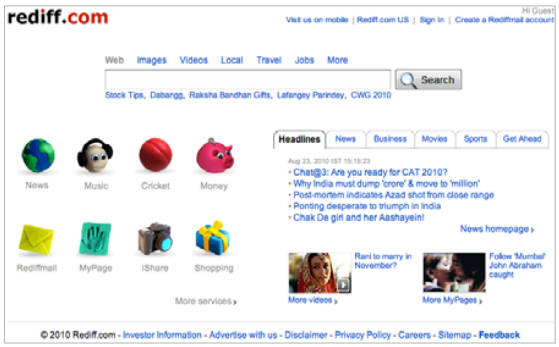

Fig. 4 RediffMail HomePage, without a Username and Password Text Box [19]

A javascript like the one given below activates a dialogue box.

document.write("<ahref=\"javascript:signin();
document.getElementById('c_uname').focus();\"
title='Already a user? Sign in'>Sign In)

Below is a screenshot of the login page of rediff.com (shown in Fig 5.).

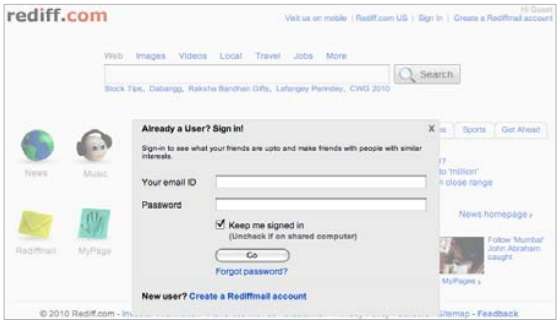

Fig. 5 Rediffmail HomePage, with a Username and Password Text Box [19]

But the most unfortunate part is that the phishers are getting smarter day by day, and they can easily include the javascript in their HTML coding to make the user believe in the fake page.

VI. Measures At The Browser End

A. Windows Internet Explorer – by Microsoft

The Microsoft Phishing Filter [20] add-in offers access to a new dynamic online service, updated several times an hour, to warn you and help protect your personal information from these fraudulent websites by firstly, scanning websites you visit and warning you if they are potentially suspicious; secondly, by dynamically checking the websites you visit with up-to-the-hour online information via an online service run by Microsoft and blocking you from sharing personal information if a site is a known phishing website.

The Microsoft Phishing Filter is integrated into Internet Explorer 7, but stays in the background until a user visits a website that looks suspicious. When a user encounters a website that looks suspicious, Internet Explorer 7 launches a dialog box asking the user to opt in [21]. Microsoft has employed a multi-pronged strategy of developing innovative technology, industry and business collaboration, and providing users and business with prescriptive guidance and tools [22].

B. Firefox – by Mozilla Corporations

By default Firefox offers a built-in feature turned on by default works by checking the site you are visiting against a known list of malicious sites. This is all based on the Google Safe Browsing Protocol (Protocolv2Spec) [23].

The first thing you should do is to install the Petname Tool add-on, which allows you to give all the protected sites you visit, pet names that are added to the cryptographic identifiers.

The biggest advantage of the Firefox is that it supports a lot of plugins, extensions, sidebars, toolbars, detector etc., to fight phishing attacks, some of them being firephish [24] and anti-phishing version 0.1.2. Another such tool is the Netcraft Toolbar add-on, which takes a very different approach to the problem. With outstanding add-ons and built-in protection, Firefox takes on phishing attacks with strength and reliability.

C. Opera – by Opera ASA Software

When Opera Fraud and Malware Protection is enabled, you contact a server at Opera once per session for each website you visit. HTTPS sites are checked via an encrypted channel, while IP addresses on the local intranet will never be checked [25]. With Opera Fraud and Malware Protection enabled, every webpage you request is subjected to phishing and malware filters. The security status of the page is displayed on the right side of the address field.

Fraud Protection includes technology from GeoTrust [26], the leading digital certificate provider, and PhishTank, a collaborative clearing house for data and information about phishing on the Internet. Fraud Protection is available in Opera 9.1, the newest version of Opera's Web browser. Opera later adds a newest functionality to our Fraud Protection feature; Malware protection [27].

D. Chrome – by Google

Phishing and malware detection is enabled by default in the

Options dialog. When enabled, Google Chrome warns you if it detects that the site you're trying to visit is suspected of phishing or containing malware. The warnings you may see when phishing and malware detection is enabled [28] may be one of the following:

1) "Warning: Visiting this site may harm your computer!"

Whenever you see this warning, Google Chrome has detected that the site you're trying to visit may contain malware. Malware is a code that attempts to steal your personal information or download harmful software onto your computer.

2) "This is probably not the site you are looking for!"

This message comes up when the URL listed in the site's certificate doesn't match the site's actual URL, which means that the site you're trying to visit may be pretending to be another site.

3) "The site's security certificate is not trusted!"

Since anyone can create a certificate, Google Chrome checks to see whether a site's certificate came from a trusted organization. This message means that the certificate wasn't issued by a recognized third-party organization.

4) "The site's security certificate has expired!" or "The server's security certificate is not yet valid!"

If you see one of these messages, that means the site's certificate is not up-to-date. Therefore, Google Chrome can't verify that the site is secure.

5) "The server's security certificate is revoked!"

The third-party organization that issued the site's certificate has marked the certificate as invalid. Therefore, Google Chrome can't verify that the site is secure.

E. Safari – by Apple Inc.

Through interaction with Google's AntiTrust database, Safari is able to automatically detect "phishy" or deceitful website URLs. It then notifies the user via a dialog box, webpage overlay, or a combination of the two. "This webpage is fraudulent. You should close it immediately," reads a dialog box that pops up in pre-release builds of the browser. "Google has identified this webpage as fraudulent. Do not enter any personal information on this page". Security enhancements protect users of Apple Computer's Safari 4.0.3 or later web browser from malicious websites.

VII. General Countermeasures

There can be many ways to fight phishing. I suggest don't just rely on a particular browser or a software (like Anti-p 2.1.0) or a anti-virus that ensures no phishing attacks but use combinations to suit your requirements.

Apart from that, you should be aware of and adopt some important techniques and methods to keep yourself safe from phishing. You should keep yourself educated about the attacks being used by attackers time to time, must change your important passwords frequently, and try to use separate passwords for different email-ids, transactions etc. You must also check the URL you are being redirected to and check for the Site's Authenticity too. I have listed some of the counter-measures I feel can be useful to you.

A. For Users:

1. The people behind OpenDNS have recently launched a site called PhishTank [29]. On this site, users can report phishing attacks. Similar Alerts can be found at FraudWatch International [30].
2. Anti-phishing toolbars are small utilities that can be quite useful in protecting a user from a known Phishing attack. Some of these toolbars that have been catching my attention include Anti-phishing Toolbar from Netcraft [31], Phishing Filter from Microsoft [32], Scamblocker from Earthlink [33], Trustwatch from Geotrust [34] and Anti-fraud Toolbar from Cloudmark [35]. SpoofGuard, EarthLink and Netcraft, were able to identify over 75% of the phishing sites tested. However, some of the toolbars were not able to identify even half the phishing sites tested [36].
3. Phishing Awareness is extremely significant for internet users. The majority of the problem lies due to the indifference of the clients in the area. The consumer advice can be taken from the Anti Phishing Working Group (APWG) [37].
4. Some common recommendation for general practices & behavior [38].

B. For Developers:

1. CipherTrust's "PhishRegistry" [39] monitors the content of your Website and alerts you when attempts to duplicate it have been detected. By registering your site on Phishregistry.org, you are able to receive notifications of online fraud attempts.
2. MarkAlert [40] is a free service offered by domaintools and can be used for domain monitoring. It involves tracking domain registrations to identify any suspicious domains which are similar sounding or use the same name or trademark as the organization which is being targeted.

3. Google's 'Inurl' and 'Intitle' advanced search [41] operators can be used to get a list of Phishing sites.

VIII. Future Developments

Inability to identify whether the website is original or not is the basic phishing problem for most users. A way out of this issue is to look at the URL and SSL certificate carefully.

However, this comes with a tremendous demand on the user's time and skill to not only analyze but also accompany it with correct judgement.

Personalizing the login page for each user is one method. A two stage login is advisable. Entering the user-id and a PIN (Personalized Identification Number) and not the password forms the first stage. This is followed by a display of a page by the server . This page is the one that shows an image which the user had selected at the time of registration. The user supplies the password only if he finds the image matching. On the other hand, if the image fails to match, an alert is raised and the user therefore does not supply the password.

For a successful log in , a login – id / static password, commonly known as PIN,and a dynamic one time password is required. The password provided to each user is generated on a hardware or a software token. These tokens automatically generate a new one time password every 60 seconds. This is a significant stage where the users will be tricked into providing their passwords at the phishing site. But the crucial point is that these passwords are valid only for 60 seconds. Failure on the part of the phisher to use it in near real time i.e. within 60 seconds, will render the password useless. However, recent proofs suggest that phishers are getting more real time and we are not fighting the real problem here.

The vital question is: *which is a better alternative – enhanced user experience at the cost of security or better security at the cost of user experience ?*

For the supporters of the former alternative, simple ways of handling phishing attacks such as personalized email communication and Improving Site Authenticity can be adopted. Alternatively, the server can generate the one-time password, instead of supplying tokens to users. On validation of the login/static password , the one time password can be generated by the server and SMSed to the user's cellphone. Since attackers can never receive this SMS, this virtually prevents phishing attacks. However, this has an important implication, namely, the need for all internet users to have mobile phones. Further, if on a travel, then with roaming facility on their cell phones each time they need to do Internet Banking. The significant question that then arises is whether the overall cost of the transaction is increasing, even if minimally so ?

The increasing loss of customer confidence in Internet commerce has been witnessed and is evident from many surveys conducted world wide in recent times. This is the challenge that is glaring in the face of most technology security experts and inspires us to find plausible, pragmatic, economic and user friendly solutions to the above.

IX. DISCUSSION

However, few enhancements to some of the existing features would include allowing users to overwrite the generated image with one of their choice (perhaps shipping with some reusable icon that the user could apply for trusted domains). One would need to be able to produce noticeably different images from different hashes. The hashes could be simple MD5 or SHA's of the domain name.

Another very interesting feature that one came across is a website of KeyScrambler [42] which boasts that even the keystrokes deep in the kernel could be encrypted. This did interest us a lot as one can look at it as a fantastic measure to combat phishing. In this the user enters the converted hashes of the password instead of the real password even in a successful phishing attempt. This would be rather useless for the phisher as the hashes can't be retraced and the password remains secure. It stays only with the user even if one is tricked into some fraud.

X. CONCLUSION

It is a cat-and-mouse game. Due to the social and human components, there are no completely effective solutions. Only through learning from our shared experiences can we hope to better protect Internet users.

Phishers are getting better every day. The security industry has taken up the challenge and today we have multiple solutions to the problem. We need to move towards effective solutions without over-burdening the user with things like personalized images during login or passwords through SMS. Only time will tell, which solutions will meet both objectives - surviving the latest attacks and finding user acceptance.

ACKNOWLEDGMENT

At the outset, in all humility, I thank the Almighty for the plentiful blessings He has showered on me to undertake and see through to completion this paper. Words are inadequate when I wish to thank my parents who have always taken pride in all my academic and educational pursuits. I wish to gratefully acknowledge the support of my sister Harshana who has been the pillar of my endeavor.

It would not be out of place to thank all the authors and researchers whose work I have consulted.. My thanks are due to the founders of the various softwares that I have used in writing this paper.

REFERENCES

[1] Wikipedia “The Free Encyclopedia”. http://en.wikipedia.org/wiki/Phishing. Accessed: April 25, 2010
[2] Anti Phishing Working Group “Global Phishing Survey: Trends and Domain Name Use in 2H2009” page. 4–5, Spring Edition, May 2010. http://www.antiphishing.org/reports/APWG_GlobalPhishingSurvey_2H2009.pdf. Accessed: June 9, 2010
[3] Anti Phishing Working Group “Phishing Activity Trends Report, 4th Quarter 2009” page. 4, October - December 2009. http://www.antiphishing.org/reports/apwg_report_Q4_2009.pdf. Accessed: June 9, 2010
[4] Personalized Sign-In Seal – Yahoo Inc. https://protect.login.yahoo.com. Accessed: May 2, 2010
[5] How do I create a sign-in seal? – Yahoo Inc. http://help.yahoo.com/l/us/yahoo/edit/privacy/edit-41.html. Accessed: June 5, 2010
[6] Sign in to Yahoo! – Yahoo Mail Homepage. https://login.yahoo.com/config/login_verify2?&.src=ym. Accessed: May 15, 2010

[7] Naveen Agarwal, Scott Renfro, Arturo Bejar – Yahoo Inc "Yahoo!'s sign-in seal and current anti-phishing solutions" page 3, Published : May 24, Oakland, California, W2SP 2007: Web 2.0 Security and Privacy 2007., in press. http://w2spconf.com/2007/papers/paper-190-z_1282.pdf. Accessed: May 22, 2010
[8] DomainKeys help detect forged email – Yahoo Inc. http://help.yahoo.com/l/us/yahoo/mail/classic/context/context-07.html. Accessed: June 13, 2010
[9] CertifiedEmail, managed by Goodmail Systems – Yahoo Inc. http://antispam.yahoo.com/certifiedemail. Accessed: June 3, 2010
[10] Google Upgrades Gmail – PC World. http://www.pcworld.com/article/118567/google_upgrades_gmail.html. Accessed: July 7, 2010
[11] Gmail preventing Phishing ! – Blog by Arjun Prabhu. http://www.arjunprabhu.com/blog/archives/2005/03/03/gmail-preventing-phishing. Accessed: July 9, 2010
[12] Spice up your inbox with colors and themes, Posted by Annie Chen, Gmail engineer – The Official Gmail Blog. http://gmailblog.blogspot.com/2008/11/spice-up-your-inbox-with-colors-and.html. Accessed: May 12, 2010
[13] The super-trustworthy, anti-phishing key, Posted by Brad Taylor, Gmail Spam Czar – The Official Gmail Blog. http://gmailblog.blogspot.com/2009/07/new-in-labs-super-trustworthy-anti.html. Accessed: May 17, 2010
[14] Choosing a smart password, Posted by Michael Santerre, Consumer Operations Associate – The Official Gmail Blog. http://gmailblog.blogspot.com/2009/10/choosing-smart-password.html. Accessed: June 13, 2010
[15] Microsoft Adds New Spam Filtering Technology Across E-Mail Platforms – Microsoft News Center. http://www.microsoft.com/presspass/features/2003/nov03/11-17spamfilter.mspx. Accessed: June 22, 2010
[16] Fighting Junk E-Mail : Hotmail Filters – Windows Live. http://mail.live.com/mail/junkemail.aspx. Accessed: June 19, 2010
[17] Don't Let Your Company Get Hooked by Phishing – Microsoft Corporation. http://www.microsoft.com/mscorp/safety/technologies/antiphishing/guidance.mspx. Accessed: June 15, 2010
[18] Sender ID Framework – Microsoft Corporation. http://www.microsoft.com/mscorp/safety/technologies/senderid/default.mspx. Accessed: June 18, 2010
[19] Homepage – Rediff.com. http://www.rediffmail.com. Accessed: July 16, 2010
[20] Microsoft Phishing Filter at a Glance – Microsoft Corporation. http://www.microsoft.com/mscorp/safety/technologies/antiphishing/at_glance.mspx. Accessed: July 12, 2010
[21] Anti-phishing White Paper – Microsoft Corporation. http://www.microsoft.com/downloads/details.aspx?FamilyId=B4022C66-99BC-4A30-9ECC-8BDEFCF0501D&displaylang=en. Accessed: July 17, 2010
[22] Microsoft's Approach to Anti-Phishing – Microsoft Corporation. http://www.microsoft.com/mscorp/safety/technologies/antiphishing/vision.mspx. Accessed: July 18, 2010
[23] Google Safe Browsing – Add-ons for Firefox. http://www.google.com/tools/firefox/safebrowsing/. Accessed: July 6, 2010
[24] FirePhish Anti-Phishing Extension – Add-ons for Firefox. https://addons.mozilla.org/en-US/firefox/addon/2366/. Accessed: July 15, 2010
[25] Opera Fraud and Malware Protection – Opera Software ASA. http://www.opera.com/docs/fraudprotection. Accessed: July 15, 2010
[26] Opera Introduces Fraud Protection, Powered by GeoTrust and PhishTank – Opera Software ASA. Accessed: July 16, 2010
[27] Malware protection – Opera Software ASA. http://my.opera.com/desktopteam/blog/2008/06/06/malware-protection. Accessed: July 16, 2010
[28] Security settings: Phishing and malware detection – Google Chrome Help. http://www.google.com/support/chrome/bin/answer.py?hl=en&answer=99020. Accessed: August 5, 2010
[29] Database for information on phishing sites reported by the public – PhishTank. http://www.phishtank.com/. Accessed: July 18, 2010
[30] Phishing Alerts – FraudWatch International. http://www.fraudwatchinternational.com/phishing/index.php. Accessed: July 19, 2010
[31] Anti-Phishing Toolbar – Netcraft. http://toolbar.netcraft.com/. Accessed: June 20, 2010
[32] Phishing Filter Add-in for MSN Search Toolbar – Microsoft Corporation. http://www.microsoft.com/mscorp/safety/technologies/antiphishing/at_glance.mspx. Accessed: June 21, 2010
[33] ScamBlocker Toolbar – Earthlink. http://www.earthlink.net/partners/sprint/software/toolbar/. Accessed: June 28, 2010
[34] TrustWatch anti-phishing service – Geotrust. http://www.geotrust.com/comcasttoolbar/. Accessed: June 27, 2010
[35] Anti – Fraud Toolbar – Cloudmark. http://www.cloudmark.com/en/home.html. Accessed: June 30, 2010
[36] Lorrie Cranor, Serge Egelman, Jason Hong, and Yue Zhang "Phinding phish: An evaluation of anti-phishing toolbars". The 14th Annual Network & Distributed System Security (NDSS) Symposium 2007 - San Diego, CA - 28th February - 2nd March., in press. http://www.isoc.org/isoc/conferences/ndss/07/papers/phinding_phish.pdf. Accessed: August 11, 2010.
[37] Anti Phishing Working Group "Consumer Advice: How to Avoid Phishing Scams". http://www.antiphishing.org/consumer_recs.html. Accessed: June 28,, 2010
[38] Mitesh Bargadiya, Vijay Chaudhari, Mohd. Ilyas Khan, Bhupendra Verma "The Web Identity Prevention: Factors to consider in the anti-phishing design", Vol. 2(7), 2010, 2807-2812, pp. 2811, ISSN: 0975-5462., in press. http://www.ijest.info/docs/IJEST10-02-07-67.pdf. Accessed: August 1, 2010
[39] TrustedSource.org, PhishRegistry.org and SpamArchive.org, Secure Computing Research Portal - CipherTrust. http://research.ciphertrust.com/. Accessed: August 16, 2010
[40] MakeAlert "Trademark and brand protection for domain names" – Domain Tools. http://www.domaintools.com/mark-alert/. Accessed: July 12, 2010
[41] Advanced Search – Google. http://www.google.co.in/advanced_search?hl=en. Accessed: August 19, 2010
[42] KeyScrambler – QFX Software. http://www.qfxsoftware.com/. Accessed: August 24, 2010

Gundeep S. Bindra (M'10) born in Kanpur, India on January 9, 1989. Bindra is pursuing the final year of Bachelor of Technology in Computer Science and Engineering from SRM University, India. The degree will be awarded in the year 2011. Bindra's major fields of study are computer networks and network securities.

He's been, as a student, an INTERN at organizations like IBM Daksh Pvt Ltd, Bangalore (India) and Jindal Stainless Ltd., Delhi (India). He has presented a Technical Paper titled – "e-Governance for Rural Development through Grid Computing", Delhi, India at the National Conference on e-Governance for Rural Development (e-GRD). His published articles include "10 Gmail Features you MUST know", India-US based online-magazine, Information Week; "11 GMail Tips you'll love!", and "5 Superpowers your GMail should have!", premier-online Indian computer magazine, PC Quest.

Mr. Bindra is a Senior Member of Indian Society for Technical Education (ISTE), Fedora Project and Computer Society of India (CSI). He also is a Mozilla Campus Representative, Mozilla Corporations., Opera Campus Crew, Opera Software ASA., Outreach College Brand Ambassador Member, My College Diary. and Outreach Member, Entrepreneurship Cell - IIT India (KGP).