International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 04 | April - 2024 SJIF Rating: 8.448 ISSN: 2582-3930

Understanding Phishing: Techniques, Detection, and Mitigation Strategies

[1]Shivam Gupta, [2]Vanika Rattan

Department of Computer Applications

Chandigarh School of Business, Jhanjeri, Mohali

Chandigarh Group of Colleges, Jhanjeri, Mohali

[1]avansh235@gmail.com

[2]vanika.rattan@gmail.com

***Abstract*—This research paper dwells in the many-sided domain of phishing and aims to provide a comprehensive view of its various dimensions. This starts from delineating the common methods of phishers such as email, SMS and voice and social engineering-based methods among others this paper tries to show how attackers leverage human psychology and technological flaws for their malicious ends. Additionally, it describes up-to-date tactics such spear-phishing email scams whaling in addition pharming that emphasize flexibility and innovativeness of malicious actors who try to elude common security mess. Effective detection mechanisms are one line of defence against these malevolent endeavours other than mere understanding of phishing techniques. This paper considers rule-based algorithms machine learning techniques anomaly detection behavioural analysis etc so as to select ones with most advantages disadvantages suitability for real-life conditions due to specific feats inherent in them. Besides detecting advanced obfuscation techniques and exploiting cognitive biases during attacks which are harder for prevention systems to identify compared simple ones because they are more complex this examination emphasizes continual enhancement of detecting tools. Detection is important but mitigation strategies are equally necessary when drumming against phishing assaults for building up digital resilience. This study examines different types of mitigation ranging from user education programs through e-mail filtering technologies, authentication proceeds involving website blacklisting up until incident response frameworks (Kruger etal., 2015). In conclusion this study offers practical recommendations on how to mitigate phishing risks and reduce their negative impact on people and organizations.**

***Keywords*—Phishing, Cybersecurity, Attack Techniques, Detection Mechanisms, Mitigation Strategies**

I. INTRODUCTION

In the modern world characterized by a boom in digital activities, phishing has emerged as a major and formidable challenge to individuals, establishments and even entire countries. Phishing is a form of cyber-attack where perpetrators disguise themselves as trustworthy bodies so as to trap victims into revealing sensitive information or carrying out dangerous operations. With an increasing dependence on digital platforms, it becomes essential to learn about various aspects of phishing practices establish effective detection mechanisms as well as implement mitigation strategies that safety in cyberspace.

II. PHISHING METHODS:

What is the same for all these different approaches used by phishers? This includes such issues as Link Manipulation: Phishing methods typically rely on some device tricks whereby an email link seems to be a link of a bogus organization itself. There are also phishers who use misspelled URLs and subdomains aswell. Consider, http://www.yourbank.example.com/, it will seem that you will be redirected to your bank website example section; however this URL points towards 'your bank' (i.e., Phishing) part of example website. Some time ago the links with "@" had been used to put passwords and user names. For example, if someone goes to http://www.google.com@members.tripod.com/, it might seem like redirection to www.google.com but actually takes browser into an actual page on members.tripod.com which uses www.google.com as the username: it opens normally regardless of the provided username.

A) *FILTER BREAKOUT:*

Anti-Phishing filters search for text commonly used in phishing emails breaching this barrier has been effected through use images of text by phisher.

B) *WEBSITE SPOOFING:*

However when someone visits a phishing site they are still vulnerable. Some Phishing scams use JavaScript commands in order to alter address bar. Either putting a legit URL over address bar or shutting down old location bar while opening new one with legit URL can do that.

C) *PHONE PHISHING:*

Bank customers received messages asking them to call up their banks due to their accounts problems. The contact number belonged to a scammer who tricked users into providing their account numbers and Personal Identification Numbers (PINs). Additionally, vPhishing (voice Phishing) would employ spoofed caller-ID data to pretend as if calls emanated from reputable organizations.

Some phishing scams utilize JavaScript codes to modify where they seem with respect to address bars on websites/ web pages. One of the ways, is inserting an image of a real URL over an address bar or simply closing down original location bar and instead opening new one that has legit URL. Another way would be if there were flaws in scripts from trusted websites visited by victims which could be potentially exploited by the attackers themselves. Examples of such attacks are cross-site scripting (XSS), where it appears to request users to sign in to their bank/service's own webpage, that is genuine throughout range from web address to security certificates; but all these facades have a link crafted for perpetrating assault so as making it almost invisible even for common user. Also, such a vulnerability was used against PayPal in 2006.

D) *COVERT REDIRECT:*

There is another type of phishing attack known as incepted redirect performed by means of links that are disguised as genuine ones but actually bring user to the attacker's webpage. In most cases, a flaw will be hidden beneath a login popup that belongs to the affected site's domain name. These vulnerabilities may also affect OAuth 2.0 and OpenID based on common exploit vectors for these vulnerabilities too. Another instance is when open redirect and XSS bugs appear on third-party application websites in use by such a service provider. It may also happen that users are secretly redirected to phishing pages courtesy of malicious browser above. When it comes to normal phish attacks, they are easy to notice since the URL of the malicious page would mostly differ from that of true site Covert redirection does not entail setting up new fraudulent sites; instead, malefactors insert faulty login popups into existing legitimate web pages. As an illustrative example, consider if a victim clicks on the Facebook beginning malicious target. So there is this Facebook popup asking whether you want to allow the app. Well should you agree, Once this is done, all your personal data including email address, birth date, contacts and work history will be transmitted directly from your computer or smartphone into hacker's hands together with "token." Furthermore, if the token has high privileges, then an

attacker can get more delicate information such as presence of mail box and friend list. What is more dangerous here concerns that attacker may now start using victims' account. A user can still get redirected even if he/she refuses allowing app. It means that the victim might refuse authorizing the rogue app yet after clicking on it they would end up in one controlled by an attacker. There is possibility that this may further endanger the subject. Mathematics Ph.D. student at School of Physical and Mathematical Sciences in Nanyang Technological University in Singapore by the name Wang Jing found out about this flaw.Though, it is not even close to being a serious matter on the Internet, covert redirect can be considered as a prominent security flaw as well as a loophole in website Open redirection attacks are viable due to some vulnerabilities existing in web applications therefore; there is an urgent need to ens these vulnerabilities are dealt with so as to reduce the number of potential phishing victims.

Over the years there have been various approaches which have been suggested on how to train users.

Human factor is wide. Teaching the end-users alone does not always control their behavior [13]. In other words, it will outline some of the work done in user training about phishing emails.

III. DETECTION OF PHISHING ATTACKS:

Because of the fact that phishing attackers target novices, it means that they can be educated to prevent their recurrence. Through many years of research and data analysis there are several ways that companies can train users who may become victims of phishing attacks.

The human factor is broad. There is need for more than just educating end users only [13]. This section will present and discuss some of the work contributed in the field of user training in relation to phishing attacks.

A. Phishing Victims Julie S Downs et al. (2014) conducted an online experiment where they sent out emails asking people for their account information such as usernames and passwords [20]. jjjThe researchers used 232 computer users who were requested to analyse email messages for potential malicious activities before answering a series questions contained therein. Results from this study indicated that individuals who knew how "phishing" was defined had a lower likelihood of falling into traps set through deceptive emails involving personal info while awareness concerning cookies, this survey has also shown that the possession of spyware as well as computer viruses did not help in reducing the vulnerability resulting from phishing emails while credit card theft awareness fails to reduce vulnerability to phishing: (Downs et al., 2007). It is important to note in this survey that knowledge about negative outcomes like credit card theft was not found to contribute significantly, which is a very interesting fact. In contrast, it was revealed that users who understood what "phishing" meant were less likely to fall prey to such tricks while data on making websites invisible did not support any correlation with vulnerability to phishing emails. Another study confirming the one in reference [20] was conducted by Huajun Huang et. al. [21] and it concluded the primary reasons that lead technology users to fall victims for phishing attacks are:

•• Users disregard passive alerts (e.g., toolbar indicators).

• Even if they were told that their capability was being assessed, many users cannot tell apart between fishing and legitimate sites. It has been shown through demographic studies conducted by Steve Shen et al that several indirect characteristics exist which tend to correlate among victims and their susceptibility towards falling prey to a phishing attack. As per their research, gender and age are highly connected with vulnerability to phishing.

They conclude that:

• Men are less likely to click on email links.

• Education programs should be targeted at the population aged 18-25 years old due to their greater likelihood of becoming victims of phishers' activities This result can be explained by lack of enough technical knowledge and experience, a notion supported by

Downset al [20] and Huang et al [21].
In their research, we have given a graphical model of the first user-phishing interaction model. The user-sketch describes how people make decisions; it starts when somebody sees an indication for phishing and ends when any action by the user occurs. This is in order to facilitate the fight against spam fishing by understanding how people relate with phishing content e.g.,

The decision-making process would be influenced by:

External information: this can either be User Interface (UI) information like Web/mail client or expert advice. Phishers can only influence what will be seen through I/O. In addition, few users request for expert opinion if not in doubt (e.g., if a user thinks a site it legitimate, he might fail to ask for expert opinion at all).

Knowledge and context: this refers to current world awareness that comes with time such as news and experiences.

Expectation: Based on their understanding of things and outcome of their activities, the users make expectations. In decision making process some two types of decisions are made Planning a series of actions to be taken.

Determining the next step to take in a sequence is based on this outcome: people are affected by previous results when moving forward. While the first action is a conscious one, subsequent actions are done subconsciously. This means that users' ability to detect phishing attacks in subsequent steps afterword's will be influenced by the outcomes of their first step. For example, such an action entails sending an email with a phony address bar URL that points to a legitimate website and then another URL pointing at a phishing site where upon logging into details like contact theft and credit card information is stolen. The first one would involve clicking on primary valid URL so as provider tries displaying an e-card it leads to 404 page not found error because it does not exist in practice . Finally, there follows clicking on backup link indicating moreover that it is easier to visit such kind of linked site more frequently than any other user who would like visiting similar sites later without being exposed thus increasing chances that one will get suspicious pausing questions upon viewing its verbal contents as viewed through eyes of potential victims targeting them up until they click or download anything else via email addressed directly to them.

For these two types of decisions:

Creating perception: perception can be created contextually such as when reading an email message. Conversation causes just as senders/recipients suggested actions by email. There exists no mismatch between what is real and what the message claims (e.g., senders in such emails are genuine and suggested actions by email content do exactly what they advise). On the other hand, while using phishing messages involves inconsistencies (for example if sender's ID seems fake or it says that it is going to fix a problem but in reality, tries to get people's personal information). Should an end-user identify some irregularities in a given phishing message then that would help him/her understand that it is a phishing attack.

Generating possible solutions: users develop solutions from available resources most times. But, with respect to phishing emails which provide solution for the user through its contents does not apply here because it includes one already. When for instance there are issues with account expiry within the content of phishing email; there will also be instructions appearing like "log in via this URL to avoid expiration."

• Setting up assessment criteria: variously different people have varied criterion for how they view things around them, their emotions etcetera; see page 3 of this paper . However, according to this article most phishing attempts do not consider those kinds of subtleties but guess on everyday common sense standards. Consider an attacker who puts a small box labeled "Sec login" so as pass security criteria needed by most users. The main aim behind many phishing attacks is achieving match

between user's and attackers' criteria; see Section 1 above . As stated before, phishers can only alter users' decision making process through UI by giving some more information. Thus, in UI there are two data sets • Content Data: That is email content or website content • Meta Data: for instance URL on the Internet address bar of a web browser or email addresses A phishing attack succeeds if users perceive that Meta data and content data is authentic.

Meta-data can also be used by users to know whether an email message is real. Details are hidden in the user interface by Phishers} {{Meta Data Content Data From: support@example.com To: client@gmail.com Subject: Account Expiry Notification Dear Client, your account will expire due to inactivity. In case you want to keep it active please login through http://PhishSite.com/activate.php. Regards, Example Inc. Technical Support. 6.User Interface (UI) components. order to further deceive the users. Consequently, educating people about these problems will never deliver substantial Metadata integrity as determining whether the source IP address was valid assuming the domain name was spoofed [5]. This means that instead of trusting individuals with validating meta, we should build this validation into the system itself.

Alternatively, cyber criminals are known to generate elaborate falsified text data using their social engineering tactics.

The awareness of how phishers work can be made by users in such instances.

IV.DETECTION OF PHISHING ATTACKS THROUGH BLACKLISTS:

Blacklists refer to lists of previously detected phishing URLs, IP addresses or keywords that are updated frequently. Conversely, whitelists could minimize F P rates because these would only accept incoming messages from trusted senders exclusively. Blacklists cannot defend against zero-hour phishing attacks since they have never been blacklisted before being identified.Blacklists have lower F P rates compared with heuristics [25]. claimed this when they said blacklists did not work on zero-day spam mails 80% of the time. In addition, this study observed that between 47% and 83% of blacklisted phishing URLs had been blacklisted in 12 hours after being identified [25]. Such a delay is significant as it encapsulates the first two hours for most phishing campaigns.

A). *GOOGLE SAFE BROWSING API*

Google Safe Browsing API allows you to check if a given URL is listed in Google's dynamic blacklist. The protocol is experimental and is built into Google Chrome and Mozilla Firefox. This is a proof-of-concept version with the two malware and phishing black lists goog-phishshavar and goog-malware-shavar respectively available from Google as the latest one. Meanwhile, the list provider does not matter to this protocol neither does its type. According to Protocolv2Spec [27], called the second implementation of this protocol (the first had scalability and efficiency issues which are also detailed in [27]), client applications should use HTTP while accessing providers' servers. Version 2 has some notable differences: • It splits URL data into chunks thereby allowing partial updates - Something impossible in version 1. • Does not always send complete hashes for blacklist URLs as aforementioned but sends a set of 32-bit truncated forms instead – Firstly, it just outputted a list with truncated hashes only for all blacklisted URLs on web browsers. However, if there existed any hash with a similar 32-bit truncated form as that contained in the truncated URLs hash list for any visited site, then all these full length 256-bit hashes whose first 'k' bits were identical to those from where they got suspecting were downloaded by the browser just afterwards. This assists in conserving bandwidths during transmission of these hash lists most especially while well aware that many times people visit authentic URLs In actuality, there is a high no-match: match ratio; thus, the first 32 bits might be sufficient (in most cases) for producing URL mismatches when different URLs are compared. Hence,

the full 256-bit URL hash will only be sent to resolve any possible hash collisions between their first 32-bits because such collisions sometimes give rise to false positives in hash functions (Protocolv2Spec [27] has more details in its Background section).

The techniques presented within this section view phishing attacks as document classification or clustering problem where machine learning models exploited by clustering algorithms like k-Nearest Neighbors (k-NN), C4.5, Support Vector Machines (SVM), k-means and DBSCAN. For example, k-NN saves the training instances that it would have represented as multi-dimensional vectors in memory with each vector component being a value from an extracted feat like number of URLs in an email message. The same is done when processing testing instances involves calculating the distance between them and other training instances say using Euclidean distance. In the case where K = 3, three classes of the nearest neighbor during the training phase are considered. When classifying majority voting on testing instance shall be used to determine its class. Unlike algorithms like k-NN which do not generalize a model, C4.5 and SVM use a different approach where they generalize classification model. For example, C4.5 constructs a decision tree that would be able to correctly classify unseen instances. It then consists nodes having branching splits that are typically made to maximize conditional Information Gain after the split. On the contrary, SVM scrutinizes all points during training process for an effective separation plane in a vector space since it aims at finding one such plane for separation purposes during prediction hence being generic enough to separate any new instance later on too .On contrast to this, unsupervised partitioning of the instances without knowing their respective class labels can be achieved by other clustering algorithms namely; Construction of k partitions with randomly chosen initial centers for these partitions is the main purpose of the K-means algorithm whose. This unit ends by assigning iterations to a partition having minimal distance (e.g., Euclidean Distance) and then it regularizes the center of the partition as an average value of instances in that particular partition. This sequence is repeated until clustering stops. On contrary, DBSCAN divides data on basis of its density that depends on how close one instance can be to another within the feature space (using some metric like Euclidean distance). Unlike K-means, DBSCAN does not need to know beforehand how many partitions to anticipate; this is determined by density reachability concept.

V. MITIGATION OF PHISHING ATTACKS:

Introduction This gives a brief introduction to the problem of phishing attacks and shows how it is possible to group various anti-phishing solutions according to their respective purposes. From our literate review, we have designed one flowchart that explains life cycle of phishing campaigns with perspective of anti-phishing techniques which serves as one of the complete flowchart for phishing solutions. The first line of defense detects when a phishing campaign has started such as sending out spam emails to users. The detection methods can be inclusive in scope and they can involve end user client software classification, service providers who use these approaches for network intrusions are protected from these methods that scan for Phishing Awareness Programs. More details in Section IV-A. When a phish campaign is detected, the knowledge acquired helps improve future detections on similar lines.For example, through studying past cases of online frauds or scams, it becomes possible to enhance fut detection mess targeting this form of cyber-crime. This kind learning may involve either human observers or some software agents under machine learning algorithms Once any attempt of phish attack is noticed there are various things that might be done with respect to such an attack .Correspondingly, there are three classifications based on our analysis: Offensive defense — pre-emptive measures that try to neutralize phishing campaigns by making them less effective than before or even useless against l users. This category offers protection especially when users have already submitted personal information such as their bank details via email to scammers or hackers pretending to be legitimate

business entities. More details are in Section IV-B.

• Correction — correction approaches mainly focus on taking down the phishing campaign. For example, either an e-mail hosting company may cancel a particular account; in relation to this, some other sites can also choose this step by contacting their internet service providers (ISPs) and requesting them not to accept any emails from those websites anymore or else blocking their IP addresses. More details in Section IV-C.

• Prevention—In literature different definitions are given for preventing phish at-tacks depending on the context but here what we mean is trying stop attackers from starting new waves of phishing campaigns. More details are in section IV-D. On the contrary if human observer or software fails to detect a phish campaign then none of these actions could be applicable…Again there's yet another reason why detection phase should be given due consideration.

A.) *Detection Approaches*

Any anti-phishing solution that helps identify or classify such attacks will therefore be referred to as detection solutions in this review.

These include:

• Approaches to user training – educating end-users on how to identify phishing attacks and distinguish them from non-phishing ones. However, in [16], user training is termed a preventive approach. Nonetheless, the user training approaches seek to improve the ability of users in detecting phishing which is why we group them under "detection". Section VI contains more discussions about the human factor.

• Approaches to software classification – these are mitigation approaches where phish and legitimate emails are classified for the users to bridge any gaps caused by human errors or ignorance. This gap is worth bridging since automated software classifiers cost less than training users on what not to click on. n some instances,However, user training and user training may not be feasible (such as when the customer base is very large e.g. PayPal, eBay). See sections VII to X for more discourse on these software classification methods.
During the training stage of a classifier whether it is human or software, classifiers work better when they are subjected to detection approaches. End-users' understanding of phishing attacks can be improved if they learn about them either by personal experiences online or even outside training programs which aim at educating users about phishing attacks like those offered by some other companies using software classifiers in Machine Learning-based classifier's learning phase or enhancing detection rules in rule based systems. These detection techniques do not only safeguard the end-users directly from being victims of phish campaigns but also improve the phishing honeypots5 used for separating phishing spam from non-phishing spam. It's worth mentioning that Mitigation of Phishing Attacks begins with Detecting them off, if you will, no other mitigation approach shall be applicable where a Phishing campaign goes undetected unlike others such as Correction Prevention and Offense Defense which all depend on an effectively functioning detection phase The main focus of this study is essentially directed towards detecting phish attacks per se.. 4 presents various kinds of approaches employed in subsequent sections. Imaging different kinds of solutions depicted in Fig

VI. Prevention Approaches:

The phrase "prevention" can be puzzling when dealing with it as applied to phishing attack because it carries various meanings depending on its context:

• Preventing users from being victims — Given this interpretation hence all techniques that detect phishes are prevention mess as well. However, this meaning does not refer here as we use "prevention".

• Preventing attackers from initiating phish campaigns — Law Enforcement Agencies (LEAs) henceforth sues attackers thereby acting as preventive mechanism.

B. *Alternative Approaches*

We can begin rectifying measures after confirming that a phish campaign has occurred. This entails taking down the phishing resources in cases of phish attacks. Service Providers are usually informed on such matters so that they respond by taking down the respective phishing resources. Several techniques are used to carry out phishing campaigns including:

• Websites — this can be a shared web host owned by a phisher, a legitimate website that has been compromised and loaded with(phishing) or multiple infected end-user workstations within a botnet6 .

• E-mail messages — these could originate from diverse sources, such as open Simple Mail Transfer Protocol (SMTP) relays, free E-mail Service Provider (ESP) like Gmail or Hotmail, or infected end-user machines which form part of a botnet.

• Social Networking services — such as Facebook and Twitter among others have become popular platforms for communication and consequently social engineering-based messages which trick users into giving away login credentials.

• User training approaches — understanding what phising is about better equips the targeted people; thus they know what is exactly phishing e-mails/communications and what is not as categorized in [16] where user training was presented as preventing method. Nonetheless, unlike preventative measures provided by [16], user training approaches are concerned with bolstering end-users' capacities to identify cyber-crime attempts called phishing thus we treat them under "detection". Later discussions related to humans will be addressed in Section VI.

CONCLUSION:

Phishing comes with various methods and tactics . Phishing involves collecting sensitive information about victims through risky links or spam messages sent to them. It becomes an important cybercrime affecting many organizations, individual gadgets etc. Phishing is at heart hacking. It comes upon many attacks that open the privacy of the user . Sometimes, it's hard to separate authentic emails from phishing ones. To beat off this attack there are some proceds that can be followed The present study presents an overview of phishing, its mechanisms, and types of such a threat.

REFERENCES:

[1]. for phishing email," J. Comput. Secur ., vol. 18, pp. 7–35, January 2010. [Online]. Available: http:// portal.acm.org/citation.cfm?id=17 34234.1734239

[2] B. Krebs, "HBGary Federal hacked by Anonymous," http: //krebsonsecurity.com/2011/02/hbgary-federal-hacked-by-anonymous/, 2011, accessed December 2011.

[3] B. Schneier, "Lockheed Martin hack linked to RSA's SecurID breach," http://www.schneier.com/blog/archives/2011/05/lockheed martin.html, 2011, accessed December 2011.

[4]. http://www.tripwire.com/

[5]. http://en.wikipedia.org/

[6]. http://webopedia.com/

[7]. http://computerworld.com/

[8] Anti-Phishing Working Group (APWG), "Phishing activity trends report — first half 2011," http://apwg.org/reports/apwg trends report h1 2011.pdf, 2011, accessed December 2011.33

[9] Anti-Phishing Working Group (APWG), "Phishing activity trends report — second half 2011," http://apwg.org/reports/apwg trends report h2 2011.pdf, 2011, accessed July – December.

[10] B. Schneier, "Details of the RSA hack," http://www.schneier.com/blog/archives/2011/08/details of the.html, 2011, accessed December

C) [11]. Kumaraguru et al., "Protecting people from phishing: the design and evaluation of an embedded training email system," in Proceedings of the SIGCHI conference on Human factors in computing systems, ser. CHI '07, 2007.

D) [12] A. Alnajim and M. Munro, "An anti-phishing approach that uses training intervention for phishing websites detection," in Proceedings of the 2009 Sixth International Conference on Information Technology: New Generations. Washington, DC, USA: IEEE Computer Society, 2009, pp. 405–410.

[13] S. Gorling, "The Myth of User Education," Proceedings of the 16th Virus Bulletin International Conference (VB'06).

[14] G. Gaffney, "The myth of the stupid user," http://www.infodesign.com.au/articles/themythofthestupiduser/, accessed March 2011.

[15] A. Stone, "Natural-language processing for intrusion detection," Computer Magazine (CM), vol. 40(12), no December , pp103-105.

[16] S Abu-Nimeh et al., "A comparison of machine learning techniques for phishing detection" in the proceedings of anti-phishing working groups 2nd annual eCrime researchers summit; ACM Press; NY; USA; p60

[17]. H.Wang and C.Yue,."Anti-phishing in offense and defense." ACSAC '08 Proceedings of the Annual Computer Security Applications Conference., vol., no., pp., .P Knickerbocker et al., Humboldt: a distributed phishing disruption system

E) [18]. Ecrime Researcher Summit ; p1

[19]. L James Phishing Exposed.. Rockland: Syngress Publishing; New York: Overdrive Inc.; Sydney: McGraw-Hill Companies Inc.; London: Pearson Education Ltd.; Boston:

J Downs et al., Behavioural response to phishing risk [20]. ACM Press; New York;

S. Liu et al., "Countermeasure techniques for deceptive phishing attack," in International Conference on New Trends in Information and Service Science, 2009, pp.636 –641.

[22] D. Moore and S. Clayton, "Examining the impact of website take-down on phishing," in Crime '07: Proceedings of the anti-phishing working groups 2nd annual Crime researchers summit; ACM Press, NY, USA; p1

[23] L Cranor et al., You've been warned: an empirical study of the effectiveness of web browser phishing warnings

F)

[24]. R Garfinkel et al., Does a security toolbar really protect against phishers?

[25] S. Sheng, B. Wardman, G. Warner, L. F. Cranor, J. Hong, and C. Zhang," An empirical analysis of phishing blacklists," in Proceedings of the 6th Conference in Email and Anti-Spam', CEAS'09, July 2009 (pp. 37-48). Abstract

[26] Google, "Google safe browsing API," http://code.google.com/apis/safebrowsing/,accessed Oct 2011.

[27] Google, "Protocolv2Spec," http://code.google.com/p/ google-safe-browsing/wiki/Protocolv2Spec, accessed Oct 2011.