Survey: Phishing Detection and Prevention Techniques in Online Banking

Priyanka Sharad Lokhande
Computer Engineering
Maharashtra Institute of Technology
Pune, India

Taranpreet Singh Saini
Computer Engineering
Maharashtra Institute of Technology
Pune, India

Nitin N. Pise
Computer Engineering
Maharashtra Institute of Technology
Pune, India

Abstract— Internet has played a major role in how we get interact with other people and how we do business. On the basis of internet, electronic commerce has been emerged, which allows business to more effectively interact with their customers and other corporations of their industries. One industry that is using this new communication channel to reach its customers is the banking industry. The unique aspect about security in banking industry is that the security posture of a bank does not depend only on the safeguards and practices implemented by the bank, but it is equally dependent on the awareness of the users regarding the use of banking channel. The task for keeping information confidentiality and integrity a greater task for the banking industry. Phishing is becoming a severe problem for users and is creating a major issue for Internet banking providers who need to find solutions to mitigate the effects of phishing to their operations. Phishing is a sort of cyber-attack where the attacker creates a replica of an existing web page to confuse users into submitting their personal, financial or password data to what they think is their service provider's website. This paper gives detail information about phishing, its attacks, its techniques and anti-phishing steps that users can take to protect their confidential information.

Keywords—e-banking; phishing; phishing detection; anti phishing techniques.

I. Introduction

1.1 ONLINE BANKING

Online banking also known as e-banking, internet banking or virtual banking, is an electronic payment system that allows customers of a bank or other financial institutions to conduct a financial transactions through the financial organization's website. The online banking systems will typically a part of the main banking system operated by a bank and is in contrast to division banking that was the traditional way customer's access banking services.

To access a financial organization's online banking facility, a customer with internet access would need to register with the organization for the service, and set up a password and other credentials for customer verification. The credentials for online banking is generally not the same as for mobile banking. Financial organizations now regularly allocate customers numbers, to check whether the customers have indicated an intention to access their online banking facility or not. Customers' numbers are usually not the same as account numbers, because the one customer number can have a number of customer accounts. The customer number can be used to access any account that the customer controls, such as cheque, savings, loan, credit card and other accounts.

The user visits the financial organization's secure website, and enters the online banking facility using the customer number and credentials which he has previously set up. The types of financial transactions which a customer could transact through online banking generally includes obtaining account balances information and list of latest transactions, electronic bill payments, and transactions between a user's or another's accounts. Some banks also allow users to download transactions directly into the user's accounting software. The facility may also enable the customer to order cheque-books, report loss of credit cards, statements, advice change of address, and other routine transactions [12].

http://dx.doi.org/10.21172/1.71.062

1.2 TYPES OF CYBER ATTACK OR THREATS FOR ONLINE BANKING

A cyber-attack is an attack on your digital systems originating from malicious acts of an unknown source. Cyber-attack allows for an illegal access to your digital device, while obtaining control of your digital device.

A different types of cyber-attacks can be defined as an violent tactic to gain an illegal access to your digital device, called the target system, originated by an attacker or a computer against a website, computer system or a single digital device as well as a whole, which becomes a risk to computer systems, information stored, and the entire network itself. Cyber-attacks compromise the integrity of the information stored and digital device.

Denial-of-Service Attack

A denial-of-service (DOS) attack means attacking the network to take it down completely by disturbing the host device which is connected to the internet. A DOS attack targets websites which are hosted on the servers of banks and credit card payment gateways [2].

Spoofing

Spoofing is a cyber-attack where a person or a program mimics another by creating false data in order to obtain illegal access to a system. Such threats are usually found in emails where the sender's address is spoofed [2].

Phishing

Phishing is a cyber-attack which makes an attempt to obtain sensitive information like passwords, usernames and other details. It is basically an email fraud where the attacker sends a legitimate looking email and attempts to gain personal information.

Trojan Horses

Trojan Horses are a form of attack that are harmful codes hidden behind genuine data which can allow complete access to the system and can affect the system or data corruption or loss of data. It acts as a backdoor and hence it can't be detected easily.

Probing

Probing is a type of attack where an attacker scans a network to obtain information or find known vulnerabilities. An attacker use map of machine and services that are available on a network can use the information to notice for exploit.

DDoS

DDoS means a Distributed Denial of Service. It is one of the ways to make any online service temporarily unavailable by generating traffic from multiple sources or services of a host connected to the internet.

1.3 TYPES OF DETECTION STRATEGIES FOR ONLINE BANKING

Digital Certificates

A public key certificate is an electronic document used to prove ownership of a public key. This certificate includes information about the key, the digital signature of an entity that has verified the certificate's contents are correct, information about its owner's identity. If the signature is valid, and the person examining the certificate faiths the signer, then they knows they can use that key to communicate with its owner.

In a public-key infrastructure (PKI) scheme, the signer is a certificate authority (CA), typically a company which charges users to issue certificates for them. In a web of trust scheme, the signer is either a self-signed certificate i.e. key owner or other users whom the person examining the certificate might know.

Certificates are an important component of Transport Layer Security (TLS), where they prevent an attacker from imitating a secure website or other server. They are also used in other applications, such as email encryption and code signing [15].

Password encryption

Now a day's one of the most important security features used are passwords. It is important for users to have secure, strong passwords. More recent Linux distributions include password programs that do not allow user to set an easily guessable password. User has to make sure the password program is up to date and has these features. There are all sorts of methods of encrypting data, each with its own set of characteristics. Most Unixes (and Linux is no exception) primarily use a one-way encryption algorithm, called DES (Data Encryption Standard) to encrypt the passwords. This encrypted password is then stored in database. When user attempt to login, the password user type in is encrypted again and compared with the entry in the file that stores the passwords. If they match, it must be the same password, it allowed access. Although DES is a two-way encryption algorithm (user can code and then decode a message, given the right keys), the variant that most Unixes use is one-way. This means that it should not be possible to reverse the encryption to get the password from the contents of database [15].

Virtual Keyboard

A machine-based keyboard is a keyboard that a client operates by making common with a group on or within a radio- or optical-detectable top or field, range rather than by very small amount physical keys. Such a system can make able the user of a small hand kept apparatus, such as a formed of small unit's telephone or a PDA (personal digital assistant) to have full keyboard power to do. In one technology, the keyboard is sent out optically on a flat top and, as the user touches the image of a key, the to do with the eye or seeing apparatus makes discovery of the bursting of blood vessel in brain and sends it to the computer. In another kind of technology, the keyboard is sent out on an area and selected keys are sent as radio signals using the short-range Bluetooth technology. Based on reasoning, with either move near, the keyboard could even be sent out in space and the user could key in by moving fingers through the air. The limited stretch of time machine-based keyboard is sometimes used to middle, half way between a soft keyboards, which appears on a viewing screen as an image map. In few cases, a software-based keyboard can be made to person's desire being dependent on the man giving food, room and so on system and special software, the user (who may be someone unable to use a regular keyboard) can use a touch screen or an instrument for pointing (for computer) to select the keys [15]. Virtual keyboard can be categorized as:

- virtual keyboards with touch screen keyboard layouts
- optically projected keyboard layouts or similar arrangements of "keys" or sensing areas
- optically detected human hand and finger motions

Secured Socket Layer

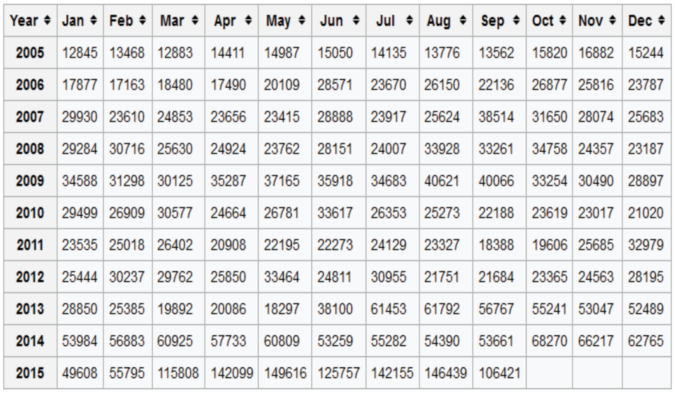
Secure Sockets Layer (SSL), is a kind of cryptographic protocol that provides communication security. Main task of SSL is to establish an encrypted link between a browser and web server. This provides integrity and data privacy of all data passed between browser and web server. SSL is an industry standard which is issued by millions of websites to protect customer's online transactions. Web server requires an SSL certificate to create an SSL connection. When any user tries to activate SSL on web server user will be driven to complete all the questions about identity of the company and website. Then two cryptographic keys are generated- a private key and a public key. The public key is kept into a certificate signing request (CSR) as it does not need to be secret. During the SSL Certificate application process. User should then submit the CSR. The Certification Authority will confirm the details and issue an SSL Certificate containing the details and permits user to use SSL. The web server will match private key with an issued SSL certificate. Then server can generate an encrypted link between the customer's web browser and the website customers can't visualize the complexity of SSL protocol. Browsers provide them with a key indicator to let them know that they are currently protected by an SSL encrypted session,- clicking on the lock icon in the lower right-hand corner displays the SSL Certificate and the details about it. SSL Certificate will contain, company name domain name, address, city, state and country, expiration date of the certificate and details of the certification authority. When a browser connects to a secure site it will retrieve the site's SSL Certificate and check that it has not expired, it has been issued by a Certification Authority the browser trusts, and that it is being used by the website for which it has been issued. If it fails on any one of these checks the browser will display a warning to the end user letting them know that the site is not secured by SSL [15].

SMS Alerts

SMS was invented from radio telegraphy in radio memo pagers using standardized phone protocols and later defined as part of Global System for Mobile Communications (GSM) as a means of sending messages of up to 160 characters to and from GSM mobile handsets. SMS stands for short message service. An SMS alert is a message sent to a cellular device, to inform the receiver of something. An SMS alert is received in the same way as a phone call is received. There are various types of SMS alerts that people may accord to. In many instances, an SMS alert is sent out to large numbers of people at once. This means that if two people receive the same SMS alert, they should receive them at about the same time. SMS alerts that contain personal information are not usually handled this way. Sending an SMS alert is often viewed by the sender as a service. There may, however, be a fee charged to both the receiver and the sender by their cellular companies [15].

II. PHISHING

Phishing is a kind of identity theft that targets to steal sensitive information from users such as credit card information, online banking passwords. Phishing attacks use a combination of technical spoofing techniques and social engineering to persuade users into giving away sensitive information (e.g., using a web form on a spoofed web page) through which attacker can make a financial profit.



Year	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
2005	12845	13468	12883	14411	14987	15050	14135	13776	13562	15820	16882	15244
2006	17877	17163	18480	17490	20109	28571	23670	26150	22136	26877	25816	23787
2007	29930	23610	24853	23656	23415	28888	23917	25624	38514	31650	28074	25683
2008	29284	30716	25630	24924	23762	28151	24007	33928	33261	34758	24357	23187
2009	34588	31298	30125	35287	37165	35918	34683	40621	40066	33254	30490	28897
2010	29499	26909	30577	24664	26781	33617	26353	25273	22188	23619	23017	21020
2011	23535	25018	26402	20908	22195	22273	24129	23327	18388	19606	25685	32979
2012	25444	30237	29762	25850	33464	24811	30955	21751	21684	23365	24563	28195
2013	28850	25385	19892	20086	18297	38100	61453	61792	56767	55241	53047	52489
2014	53984	56883	60925	57733	60809	53259	55282	54390	53661	68270	66217	62765
2015	49608	55795	115808	142099	149616	125757	142155	146439	106421			

Total number of unique phishing reports (campaigns) received

According to Ghosh, there were "445,004 attacks in 2012 as compared to 258,461 in 2011 and 187,203 in 2010", showing that phishing has been increasingly threatening individuals [10].

2.1 PHISHING TYPES

Phishing

An attempt to obtain information such as passwords, username and credit card details by masked as an honest entity in an electronic communication. In October 2013, emails claiming to be from American Express were sent to an unknown number of recipients. A DNS change could have been made to ruin this spoofed email, but American Express failed to make any changes.

Spear phishing

Phishing attempts focused at specific individuals or companies have been termed spear phishing. Attackers may collect personal information about their target to get more success. This technique is the most successful on the internet, accounting for 91% of attacks [17].

Clone phishing

Clone phishing is an attack whereby a genuine, and formerly delivered, email containing an attachment had recipient address taken and its content and used to create an almost identical email. The link within the email is replaced with a nasty version and then sent from an email address deceived to appear to come from the original sender. It may claim to resending of the original or an updated version to the original. This technique can be used to pivot from a previously infected machine and gain a position on another machine, by misusing the social trust associated with the contingent connection due to both parties getting the original email [17].

Whaling

Some recent phishing attacks have been focused specifically at senior executives and other high profile targets within businesses, and the term whaling has been invented for these kinds of attacks. In the case of whaling, the masked web page will take a more serious executive-level form. The content will be created to target an upper manager and the individual's role in the company. The content of a whaling attack email is often written as a legal order, customer complaint, or executive issue. Whaling scam emails are intended to masquerade as a critical business email, sent from a genuine business authority. The content is meant to be personalized for upper management, and usually involves some kind of untrue company-wide concern. Whaling phisher men have also forged official-looking FBI subpoena emails, and claimed that the manager needs to click the link and install special software to view the subpoena [17].

2.2 PHISHING CLASSIFICATION

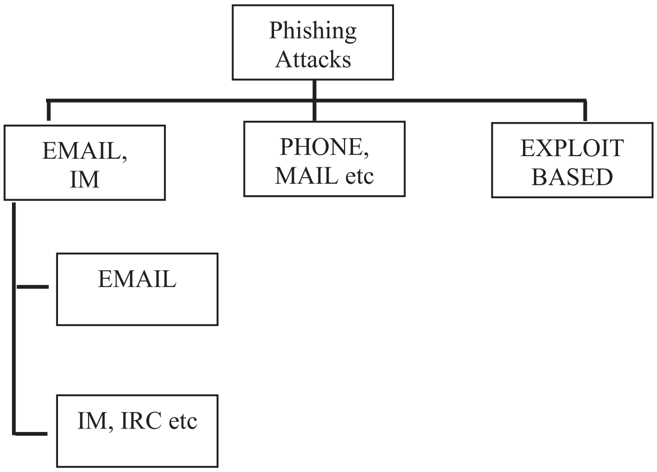


FIG. 1 PHISHING CLASSIFICATION

2.3 PHISHING TECHNIQUES

Web Spoofing

Web Spoofing is a type of security attack that allows an opponent to observe and change all web pages sent to the victim's machine, and observe all information entered into forms by the victim. Web Spoofing works on both of the major browsers and is not prevented by "secure" connections. The attacker can detect and modify all web pages and form submissions, even when the browser's "secure connection" indicator is lit. The user sees no indication that anything is wrong.

Once this information is collected, the attacker can use it to buy things with the victims' credit cards, access their bank accounts, and establish false identities. Website spoofing is a growing phenomenon, and puts consumers at considerable risk for identity theft and credit card fraud.

The attack is initiated when the victim visits a malicious Web page, or receives a malicious email message (if the victim uses an HTML-enabled email reader) [17].

E-mail spoofing

Email spoofing is an action in which the sender address and other parts of the email header are altered to appear as though the email created from a different source. Because central SMTP doesn't provide any authentication, it is easy to mimic and forge emails. Distributors of spam often use spoofing in an attempt to get recipients to open, and possibly even respond to, their application. Spoofing can be used legally. Classic examples of senders who might prefer to cover-up the source of the e-mail include a sender reporting neglect by a spouse to a welfare agency who fears revenge [17].

2.4 PHISHING PROCESS

In a classic phishing, the attackers send a large amount of spooled emails to number of internet customers that seem to be coming from a genuine society. Email wishes to provide delicate information. By clicking on the link provided in the e-mail, user is directed to a fake site made by the attacker [18].

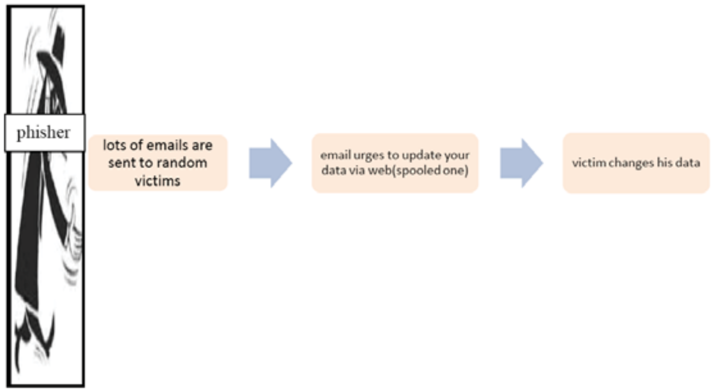

phisher
lots of emails are sent to random victims
email urges to update your data via web(spooled one)
victim changes his data

FIG. 2 PHISHING PROCESS

2.5 ANTI PHISHING TECHNIQUES

There are many answers developed to battle the phishing attacks. It includes both technical and non-technical areas. Yet, the tendency of phishing is increasing and the numbers of new techniques are implemented to cause more harm, it's becoming a serious cybercriminal activity.

Anti-Phishing Prevention Technique namely APPT is based on the concept of avoiding phishing attacks by using combination of one time password and encrypted token for user machine identification. First step is to gain the password by SMS or by emails, during that process encrypted token is produced which have user exact data and is kept in the user machine. Second step is to access the essential website with the password and valid token which are required for successful verification. This Section presents the implementation and how it can help in justifying a typical phishing attempt [18].

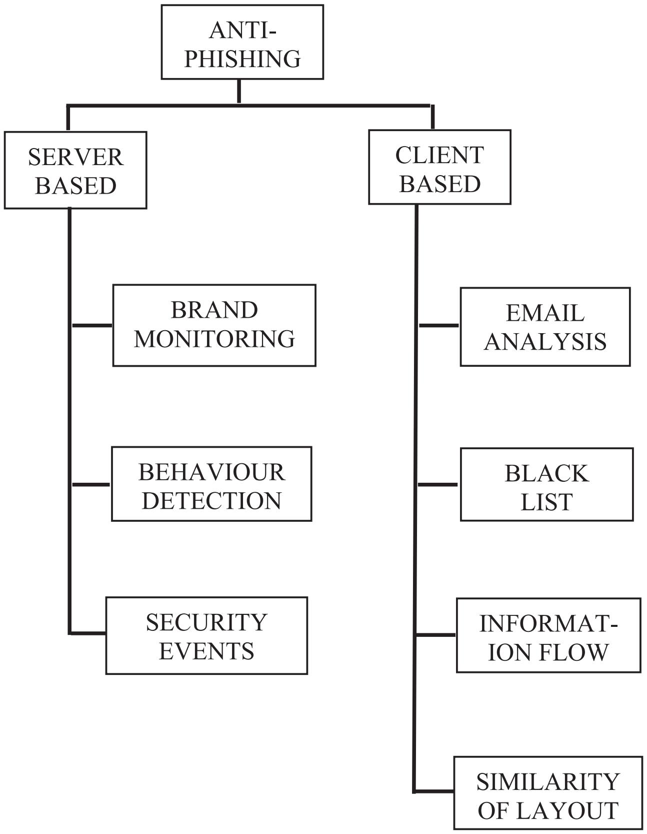


FIG. 3 ANTI PHISHING TECHNIQUES

SERVER BASED - these techniques are implemented by service providers (ISP, etc) and are of following types:

- Brand Monitoring - Cloning online websites to identify “clones” which are considered phishing pages. Suspected websites are added to centralized “black list”.
- Behavior Detection - for each customer, a profile is identified (after a training period) which is used to detect anomalies in the behavior of users.
- Security Events - Security event analysis and correlation using registered events provided by several sources (OS, application, network device) to identify anomalous activity or for post mortem analysis following an attack or a fraud.

CLIENT BASED - these techniques are implemented on user’s end point through browser plug-ins or email clients and are of following types:

- Email Analysis - Email based approaches typically use filters and content analysis. If trained regularly, Bayesian filters are actually quite effective in intercepting both spamming and phishing e-mails.
- Black List - Black lists are collection of urls identified as malicious. The black-list is queried by the browser at run time whenever a page is loaded. If the currently visited url is included in the black list, the user is advised of the danger otherwise the page is considered legitimate.
- Information Flow - Information flow solutions are based on the premise that while a user can be easily fooled by URL obfuscation or a fake domain name, a program will not run. Anti-Phish is an example of this type of technique which keeps track of sensitive information that the user enters into web forms, raising an alert if something is considered unsafe.
- Similarity of Layout - Most advanced techniques try to distinguish a phishing page from a legitimate page by comparing their visual similarities. DOM-Anti-phish computes the similarity value extracting the DOM-tree of the considered WebPages [18].

Other than client based and server based techniques; we can also use the technique of one time password (OTP). A one-time password (OTP) is a password that is valid for only one login session or transaction, on a computer system or other digital device. OTPs avoid a number of shortcomings that are associated with traditional (static) password-based authentication; a number of implementations also incorporate two factor authentication by ensuring that the one-time password requires access to something a person has (such as a small keying fob device with the OTP calculator built into it, or a smartcard or specific cell phone) as well as something a person knows (such as a PIN).

The most important advantage that is addressed by OTPs is that, in contrast to static passwords, they are not vulnerable to replay attacks. This means that a potential intruder who manages to record an OTP that was already used to log into a service or to conduct a transaction will not be able to abuse it, since it will no longer be valid. A second major advantage is that a user, who uses the same (or similar) password for multiple systems, is not made vulnerable on all of them, if the password for one of these is gained by an attacker. A number of OTP systems also aim to ensure that a session cannot easily be intercepted or impersonated without knowledge of unpredictable data created during the previous session, thus reducing the attack surface further [24].

2.6 APPROACHES FOR ANTI-PHISHING

We briefly review the approaches for anti-phishing:

- *Detect and block the phishing Web sites in time:*
  Detecting phishing web sites in time, we can then block the websites and can easily prevent the phishing attacks. It is easy to check (manually) whether the website is phishing or not, but it is then difficult to find those phishing sites out in time. Following are the two phishing site detection methods [9].
- *Enhance the security of the web sites:*
  Many commercial and banking sites can use new methods to fix the security issue of user’s personal information. One major method is to use hardware devices. And other method is to use the biometric devices like voice, fingerprints, iris detection etc. for easy authentication of the customer [9].
- *Block the phishing e-mails by various spam filters:*
  The online criminals generally use e-mails as their best trap to fetch user personal information. To deliver e-mails we use the protocol of SMTP that is simple mail transfer protocol. It is the basic protocol which lacks in the security and the necessary authentication mechanism. Information related to sender, like name and e-mail address of the sender, message route etc. can be easily changed in simple mail transfer protocol. Therefore, attackers can send large number of fooled e-mails which are seemed

to be legitimate organizations. The online criminals hide their identities when they send these kind of e-mails. If the anti-phishing system can determine that whether e-mail is sent by the announced sender, then the phishing attacks will be decreased automatically [9].

- *Install online anti-phishing software in user's computers:* Instead of all the above attacks, it is still possible for the customers to visit the spoofed websites. At last defense, users can use anti-phishing tools and install them in their computers. The anti-phishing tools used today are divided in two categories: blacklist/white list based and rule based category [9].

III. FUTURE WORK

In future the technology should be more encrypted and secure and it must be difficult to break. Clients also have to be aware of online risks in banking sector and should use the internet responsibly.

Phishing is increasing with great rate in this sector and it has also increased in number of types as discussed in the paper, so industry people should start to protect users with appropriate security structures. Industry people should also aware people about phishing with appropriate knowledge and by training them, so that they cannot be trapped in this problem.

People can also do more work on server side security and in this type of security; we can use dual level of protection or authentication for the customers to access their account easily. Most important thing is that to educate the customers about these policies by banks so that customers start using online banking service more frequently without any fear of phishing problem.

IV. ACKNOWLEDGEMENT

We would like to thank our ME Coordinator Prof. Nitin N. Pise (Non-Credit Course) for sharing their pearls of wisdom with us during the course of this research.

V. CONCLUSION

Phishing is the major law breaker in the field of online banking transactions, with number of false e-mail phishing attacks on many innocent users being trapped in last few years. Inappropriately many users end up by giving their personal information to the online criminals, resulting in many emotional and financial losses. Many anti-phishing techniques have been formed to protect users from phishing. But apart from these counter-measures on phishing preventions, main aim of the industry people is to educate their users on the risks to reduce the phishing attacks on online banking users. This paper mainly focuses on the proper awareness and education of the phishing and anti-phishing preventions to minimize the negative effects on online bank customers and therefore it may regain the trust of the customers again in this innovative banking channel.

REFERENCES

[1] J. Eom, N. Kim, and S. Kim, "Cyber Military Strategy for Cyberspace Superiority in Cyber warfare," pp. 295–299.

[2] J. Raiyn and B. Alqarbiah, "A survey of Cyber Attack Detection Strategies," vol. 8, no. 1, pp. 247–255, 2014.

[3] I. M. Journal, "Law mantra," vol. 2, no. 7, 2014.

[4] A. Shukla and L. Gehlod, "A survey on phishing detection and prevention technique," vol. 3, no. 5, pp. 6255–6259, 2014.

[5] S. Rehman, "Impact of Electronic crime in Indian Banking Sector – An Overview," no. 2, pp. 159–164, 2011.

[6] E. S. Rosengren, "Financial Stability "," 2015.

[7] A. Bamrara, G. Singh, and M. Bhatt, "Cyber Attacks and Defense Strategies in India : An Empirical Assessment of Banking Sector," vol. 7, no. 1, pp. 49–61, 2013.

[8] T. H. E. Defence and C. Strategy, "The defence cyber strategy."

[9] E. K. Reddy and M. V. V. Saradhi, "DETECTION OF E-BANKING PHISHING WEBSITES," vol. 2, no. 1, pp. 46–54.

[10] https://en.wikipedia.org/wiki/Phishing

[11] G. Pathak, R. Nishar, H. Shah, and P. Gajera, "Study of Anti- Phishing on Internet Banking," vol. 2, no. 2, pp. 195–197, 2015.

[12] https://en.wikipedia.org/wiki/Online_banking

[13] E. U. Agency and I. Security, *Network and Information Security in the Finance Sector*, no. December. 2014.

[14] C. S. Oehmen, E. Al-shaer, and M. Rahman, "Automated Decision Making for Active Cyber Defense : Panel Discussion," p. 2809828, 2015.

[15] S. C. Bhatt, "Study of Indian Banks Websites for Cyber Crime Safety Mechanism," vol. 2, no. 10, pp. 87–90, 2011.

[16] E. Kirda and C. Kruegel, "Protecting Users Against Phishing Attacks with AntiPhish."

[17] A. A. Khan, "Preventing Phishing Attacks using One Time Password and User Machine Identification," vol. 68, no. 3, pp. 7–11, 2013.

[18] J. Chhikara and M. Rani, "International Journal of Advanced Research in Phishing & Anti-Phishing Techniques : Case Study Phishing attacks Exploit Based," vol. 3, no. 5, pp. 458–465, 2013.

[19] G. Goh, G. Gan, T. N. Ling, G. C. Yih, and U. C. Eze, "Phishing : A Growing Challenge for Internet Banking Providers in Malaysia," vol. 5, pp. 133–142, 2008.

[20] "Interested in learning more ? Phishing for Banks ull rig ht In sti tu te ho," no. Security 401.

[21] R. K. Jassal and R. K. Sehgal, "Study of Online Banking Security Mechanism in India : Take ICICI Bank as an Example," vol. 13, no. 1, pp. 114–121, 2013.

[22] N. P. Singh, M. Road, D. Warehouse, D. Mining, and E. Projects, "Journal of Internet Banking and Commerce," vol. 12, no. 2, 2007.

[23] R. K. Jassal, "Online Banking Security Flaws : A Study," vol. 3, no. 8, pp. 1016–1021, 2013.

[24] https://en.wikipedia.org/wiki/One-time_password