Phishing Scams in India and Legal Provisions

The media runs stories on an almost daily basis covering the latest bank to have their customers targeted and how many victims succumbed to the attack. It may be you too. Suppose, one day you open your email, and found a weird looking mail, something phisy! A message in your inbox from your bank with which you have an internet enabled account asking to update your account with your personal information, login detail etc. on pretext of up gradation of server of the bank. You would also see a link, by clicking on which you would be linked to a look alike website of your bank which looks quite authentic and convincing. However, you may be smart enough to know that this is a trap by a con to get your vital personal information to make fraudulent financial transactions and swindle your money. But there are many others who are not as smart as you, and fall into the trap and pass on their vital login details and lose their valuable money.

Phishing is the internet age crime, born out of the technological advances in internet age. "Phishing" is a newer form of social engineering. Typically, Phishing is a form of social engineering, characterized by attempts to fraudulently acquire sensitive information, such as passwords, usernames, login IDs, ATM PINs and credit card details, by masquerading as a trustworthy person or business in an apparently official electronic communication, such as an email or an instant message. The phishing attacks will then direct the recipient to a web page (mirror webpage) so exactly designed to look as a impersonated organization's (often bank & financial institution) own website and then they cleverly harvest the user's personal information, often leaving the victim unaware of the attack.

Phishing has become so rampant that even, the Oxford English Dictionary added "Phishing" to its latest publication making it a definitive word of English Language. It defines "Phishing" as:

"phishing *• noun the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers, online."*

As per the American Banker's Association "*Phishing attacks use 'spoofed' e-mails and fraudulent Web sites designed to fool recipients into divulging personal financial data such as credit card numbers, account usernames and passwords, Social Security numbers, etc. By hijacking the trusted brands of well-known banks, online retailers and credit card companies, phishers are able to convince up to 5 percent of recipients to respond to them."*

The Anti-Phishing Working Group (APWG) which is an industry association focused on eliminating identity theft and fraud from the growing problem of phishing and email spoofing defines Phishing as a form of online identity theft that employs both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials.

According to the Annual Report of the Indian Computer Emergency Response Team (CERT-In), Deptt. of Information Technology, Ministry of Communications & Information Technology, (Govt. of India) in the year 2009, the CERT-In handled about 374 phishing incidents.

Major factors for increase in Phishing Attacks:

There are three major factors behind the recent spurt in phishing attacks worldwide particularly in India:

Unawareness among public: Worldwide, particularly in India, there has been lack of awareness regarding the phishing attacks among the common masses. The users are unaware that their personal information is actively being targeted by criminals and they do not take proper precautions when they conduct online activities.

Unawareness of policy – The fraudsters often count on victim's unawareness of Bank/financial institution policies and procedures for contacting customers, particularly for issues relating to account maintenance and fraud investigation. Customers unaware of the policies of an online transaction are likely to be more susceptible to the social engineering aspect of a phishing scam, regardless of technical sophistication.

Technical sophistication – Fraudsters are now using advanced technology that has been successfully used for activities such as spam, distributed denial of service (DDoS), and electronic surveillance. Even as customers are becoming aware of phishing, criminals are developing techniques to counter this awareness. These techniques include URL obfuscation to make phishing emails and web sites appear more legitimate, and exploitation of vulnerabilities in web browsers that allow the download and execution of malicious code from a hostile web site.

Techniques of Phishing attacks

Man-in-the-middle attacks: In this class of attack, the attacker sits between the customer and the real web-based application, and proxies all communications between the systems. This form of attack is successful for both HTTP and HTTPS communications. The customer connects to the attackers server as if it was the real site, while the attackers server makes a simultaneous connection to the real site. The attackers server then proxies all communications between the customer and the real web-based application server – typically in real-time.

URL Obfuscation Attacks: Using URL obfuscation techniques which involves minor changes to the URL, the fraudster tricks the user to follow a hyperlink (URL) to the attacker's server, without the users realizing that he has been duped. URL Obfuscation uses the unspoken, unwritten secrets of the TCP/IP protocol to trick users into viewing a website that they did not intend to visit.

XSS (Cross-site Scripting): Cross-site scripting attacks (XSS) make use of custom URL or code injection into a valid web-based application URL or imbedded data field. In general, these XSS techniques are the result of failure of a site to validate user input before returning it to the client's web-browser.
Phishing scenario in XSS:

- Victim logs into a web site
- Attacker has spread "mines" using an XSS vulnerability
- Victim fall upon an XSS mine
- Victim gets a message saying that their session has terminated, and they have to to authenticate again
- Victim's username and password are send to attacker

Some cases of phishing in India:

Phishing is a relatively new concept in India, unheard of couple of years back but recently there has been rise in the number of phishing cases in India where the innocent public fall prey to the sinister design of fraudster. In India, the most common form of phishing is by email pretending to be from a bank, where the sinister asks to confirm your personal information/login detail for some made up reason like bank is going to upgrade its server. Needless to say, the email contains a link to fake website that looks exactly like the genuine site. The gullible customers thinking that it is from the bank, enter the information asked for and send it into the hands of identity thieves.

There were phishing attempts over ICICI Bank, UTI Bank, HDFC Bank, SBI etc. in which the Modus operandi was similar. It was reported that a large number of customers of these banks had received emails, which have falsely been misrepresented to have been originated from their bank. The recipients of the mails were told to update their bank account information on some pretext. These emails included a hyperlink with-in the email itself and a click to that link took recipients to a web page, which was identical to their bank's web page. Some of the unsuspecting recipients responded to these mails and gave their login information and passwords. Later on, through internet banking and by using the information so collected a large number of illegal/fraudulent transactions took place.

Apart from the general banking phishing scams, some of the recent phishing attacks that took place in India are as follows:

- **RBI Phishing Scam:** In a daring phishing attack of its kind, the fraudsters even have not spared the Reserve Bank of India. The phishing email disguised as originating from the RBI, promised its recipient prize money of Rs.10 Lakhs within 48 hours, by giving a link which leads the user to a website that resembles the official website of RBI with the similar logo and web address. The user is then asked to reveal his personal information like password, I-pin number and savings account number. However, the RBI posted a warning regarding the fraudulent phishing e-mail on the bank's official website.
- **IT Department Phishing Scam**: The email purporting to be coming from the Income Tax Department lures the user that he is eligible for the income tax refund based on his last annual calculation, and seeks PAN CARD Number or Credit Card details.
- **ICC World Cup 2011**: One of the biggest sporting events is also under phishing attack. The fraudsters have specifically targeted the internet users of the host countries i.e. India, Bangladesh and Sri Lanka where the matches of the world cup are going on. India, which has been allotted 29 matches of the world cup, is obviously the prime targets of the phishing attacks. The Modus Operandi is similar to the banking phishing attack. The fraudsters through the similar looking fake website of organizers of the event have tried to lure victims with special offers and packages for the grand finale of the event. The Users were asked for credit card details to book tickets and packages along with their personal information which once submitted would be used to compromise the online banking account of the victim leading to financial losses to the victim.
- **Google under Phishing Attack**: Recently, the users of the Google email services, "Gmail" purportedly received a legal notice from the Gmail team which wanted users to refurbish their account name, password, occupation, birth date and country of residence with a warning that users who did not update their details within 7 days of receiving the warning would lose their account permanently. However, the

spokesperson of the Google denied any such legal notice coming from them and stated it to be a phishing attack designed to collect personal information, called 'spoofing' or 'password phishing'.

Modus Operandi of phishing attack used to target bank customers in India:-

1. The hackers have created a fake look alike websites of the target Bank or the organization and sent emails to the customers of the bank/organization luring them to provide them the login details in order to upgrade the server. It was revealed that for this purpose the fraudster hosted the web page containing URL Links of the target bank/organization with the help of their associates from foreign countries like Nigeria, Russia etc.
2. Before a transfer of funds through internet banking is executed, the bank sends a SMS to the transferor in order to confirm the transaction. The fraudsters, when they get hold of the customer's personal information changed the contact numbers of customers with their own, so that the transfer of funds through victim account to beneficiary accounts goes unnoticed.
3. In these cases, when the customers fell into trap and passed on their Internet banking password and user name, the fraud was perpetuated in three forms:-
    a) The account to account transfer from1 the victim's account to a beneficiary account.
    b) For recharging the mobile phones.
    c) Making purchases online permissible by net banking facility.
4. The beneficiary account in which the funds were transferred were fake accounts which were opened by giving fake ID documents, like fake passports, fake election I Cards, Fake Pan Cards etc.
5. The phishing scam revealed the involvement of Nigerians but the beneficiary accounts were opened in the name of Indians as the account with Nigerian names would arouse suspicion. Some of the beneficiary account holders were carrier of the hackers while some of the beneficiary's accounts were opened by luring the persons by giving them some consideration in lieu of their services to open the account in their names and get the ill-gotten money transferred in their accounts.
6. The suspected IP addresses from which the fraudulent internet transaction took place were of various foreign countries which indicate the use of proxy IPs by the hackers to mislead the investigation agencies.
7. It has been revealed that the amount has been withdrawn immediately by the hacker after the account has been compromised.

Phishing-A Cyber Crime, the provisions of Information Technology Act, 2000

The phishing fraud is an online fraud in which the fraudster disguise themselves and use false and fraudulent websites of bank and other financial institutions, URL Links to deceive people into disclosing valuable personal data, later on which is used to swindle money from victim account. Thus, essentially it is a cyber crime and it attracts many penal provisions of the Information Technology Act, 2000 as amended in 2008 adding some new provisions to deal with the phishing activity. The following Sections of the Information Technology Act, 2000 are applicable to the Phishing Activity:

Section 66: The account of the victim is compromised by the phisher which is not possible unless & until the fraudster fraudulently effects some changes by way of deletion or alteration of information/data electronically in the account of the victim residing in the bank server. Thus, this act is squarely covered and punishable u/s 66 IT Act.

Section 66A: The disguised email containing the fake link of the bank or organization is used to deceive or to mislead the recipient about the origin of such email and thus, it clearly attracts the provisions of Section 66A IT Act, 2000.

Section 66C: In the phishing email, the fraudster disguises himself as the real banker and uses the unique identifying feature of the bank or organization say Logo, trademark etc. and thus, clearly attracts the provision of Section 66C IT Act, 2000.

Section 66D: The fraudsters through the use of the phishing email containing the link to the fake website of the bank or organizations personates the Bank or financial institutions to cheat upon the innocent persons, thus the offence under Section 66D too is attracted.

The Information Technology Act, 2000 makes penal provisions under the Chapter XI of the Act and further, Section 81 of the IT Act, 2000 contains a non obstante clause, i.e. "the provisions of this Act shall have effect notwithstanding anything inconsistent therewith contained in any other law for the time being in force". The said non obstante clause gives an overriding effect to the provisions of the IT Act over the other Acts including the Indian Penal Code. The aforesaid penal provisions of the IT Act, 2000 which is attracted to the phishing scam are however been made bailable by virtue of Section 77B IT Act intentionally in view of the fact that there is always an identity conflict as to the correct or accurate identity of the person behind the alleged phishing scam and there is always a smokescreen behind the alleged crime as to the identity of the person who has actually via these online computer resources have or have not committed the offence and in view of the possible misuse of the penal provision for cyber offences as contained in the IT Act, the offence is made bailable.

What Should Internet Users Do About Phishing Schemes?

With online transactions on rise, certain precautionary measures are to be taken by all those who make their transactions online, like credit card holders, internet bank users, to shield themselves from such frauds. Some of the precautionary measures are as follows:-

1) The US Department of Justice recommends the user to follow a golden rule what is known as Stop, Look & Call (SLC). The SLC rule emphasizes that:-
    a. You must STOP because the phishing emails are always desperate in their language and so eager to retrieve information from you. It generally comes with a warning you give the personal information or else your account would be deactivated. Be automatically suspicious of any email with urgent/desperate requests for personal financial information.
    b. You must LOOK because the link provided in the phishing email is a fake URL and by using your sixth sense, you would see that email address itself is bogus. For example, an email which purportedly come from UTI Bank might be UTI.Bank @ yahoo.com which obviously is not the original email address of UTI Bank.
    c. You must CALL because in case you find the email suspicious & even if you don't fall into the trap, it should be your endeavor as a good citizen to inform the target bank and the law enforcement agencies so that timely action should be taken to save other customers from being trapped by the fraudster.

2) Check your credit card and bank account statements regularly and look for unauthorized transactions, even small ones. Report discrepancies immediately
3) Ensure that your system has the current security software applications like; anti-spam, anti-phishing, anti-virus and anti-spyware etc.

What do you do if you think you are a victim?

- If you have provided account numbers, pin number, password, login detail to the phisher, immediately notify the bank with which you have the account so that your accounts can't be compromised.
- Even if you don't fall into the trap, it is your duty as a good citizen to avoid others from falling into the trap. You should report phishing to bank or agency that was being impersonated as well as to police.

Phishing is a major concern in the contemporary e-commerce environment in India and will continue to be so because of the lack of awareness among the Internet users who are new to the internet realm. There is no silver bullet to thwart the phishing attack. However, it has been noticed in the most of the phishing scams worldwide particularly in India that the hacker succeeds in phishing attempt due to the uninformed, gullible customers who without knowing that they are being trapped unwittingly pass on the information asked for by the fraudster. Therefore, the awareness and customer education is the key here to fight the menace of the "Phishing" apart from mitigating or preventative measures. The law enforcement agencies, the legislature, the industry should come together and coordinate in their fight against the menace of the Phishing.

Neeraj Aarora
AICWA, LLB, MIMA, PGD (Cyber Law), CFE
Advocate