Phishing and Its Indian Perspective

B Bhagat, L Kharb

Citation

B Bhagat, L Kharb. *Phishing and Its Indian Perspective*. The Internet Journal of Medical Informatics. 2007 Volume 3 Number 2.

Abstract

The advent of Internet has provided a remarkable platform for individual-to-individual communication. This has enabled a person to share things with people at far way places i.e one can make new friends, share their files & experiences, buy things from stores without actually visiting them and so on. But like every other coin, this atypical method of inter-personal contact has the other side too. Persons with criminal bent of mind have found a way of targeting victims without actually meeting them and with the least risk of being caught. One such crime that is gaining momentum these days is called “Phishing”.

INTRODUCTION : PHISHING

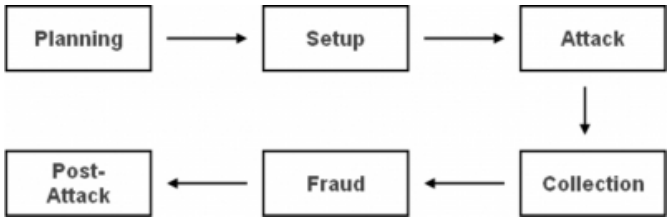
Phishing is a form of social engineering in which an attacker attempts to fraudulently acquire sensitive information from a victim by impersonating a trustworthy third party, which could be a person or a reputed business in an electronic communication. The objective is to trick recipients into divulging sensitive information such as bank account numbers, passwords and credit card details. For instance, a phisher misrepresenting himself as a large banking corporation or popular on-line auction site will have a reasonable yield, despite knowing little to nothing about the recipient. A person engaged in phishing activities is called a phisher. Phishing attacks today typically employ generalized “lures”, intimidating users and creating fear – a common example is “we need you to confirm your account details or we must shut your account down”. An approach which is believed to become more and more common is context aware attack: this is a more complex approach as it not only uses threat or enticement, but makes the victim think of the messages as expected, and therefore legitimate. The method used by phishers is usually to make fraudulent websites, similar to the genuine website by mimicking the HTML code containing the same images, text and sections. Some phishing websites register a similar domain name to the legitimate website of a company or a bank. The most common method used by phishers is by forms, for example, the Internet Banking login page or a form for password verification. Many phishing attempts use domain spoofing or homographic attacks (Gabrilovich & Gontmakher, 2002) as a step towards persuading victims to give out personal information. A phisher could target many kinds of confidential information, including user names and passwords, credit card numbers, bank account numbers, and other personal information. In a study by Gartner (Gartner Inc, 2004), about 19% of all those surveyed reported having clicked on a link in a phishing email, and 3% admitted to giving up financial or personal information.

A common phishing attack is (for a phisher) to obtain a victim's authentication information corresponding to one website (that is corrupted by the attacker) and then use this at another site. This is a meaningful attack given that many computer users reuse passwords – whether in verbatim or with only slight modifications. The phishing attack lifecycle can be decomposed in :

- Planning,
- Setup,
- Attack,
- Collection,
- Fraud and
- Post-Attack Actions.

Figure 1

Figure 1: Phishing attack lifecycle



Phishing includes many different types of attacks like,

- Deceptive attacks, in which users are tricked by fraudulent messages into giving out information;
- Malware attacks in which malicious software causes data compromises; and
- DNS-based attacks in which the lookup of host names is altered to send users to a fraudulent server. (Emigh, 2005).

A successful phishing attempt is likely to affect three kinds of people, the receiver, the Internet Service Provider and the bank or the company on whose name the fraudulent mails are sent. The receiver is at the risk of compromising his/her personal information like credit card details, social security number, etc. The Internet Service Provider suffers as thousands of mails are sent in the fishing scam, thus clogging its network and bringing down the revenues. The bank/company targeted is at the risk of losing its brand image, customer loyalty and future business. (Emigh, 2005).

STEPS IN A TYPICAL PHISHING ATTACK

The phisher plans the attack, creates the attack code/message and sends to the target user. A malicious message arrives at the target site. The ignorant target reads the message and takes some action which makes him or her vulnerable to an information compromise. The user is then prompted for confidential information through a familiar and trustworthy looking web interface. The user reveals his confidential information. The confidential information is transmitted from a phishing server to the phisher. The phisher engages in fraud using confidential information to impersonate the user.

There is no single way that can prevent all phishing. But different methods applied at different stages of phishing attack can abort a phishing attempt and properly applied technology can significantly reduce the risk of identity theft. (Emigh, 2005).

In an attack on Google.com, users were redirected to a spoofed copy of Google's front page with a large message claiming “You WON $400.00 !!!”. Users were presented with instructions for collecting their prize money. These instructions direct users to enter their credit card number and shipping address. Once the information has been collected and stolen, users were then seamlessly directed to Google's legitimate website. (Anti-Phishing Working Group, 2005). A study on number of new phishing sites formed world over in a given year revealed that there is a progressive trend with 3326 in May 2005 to 11976 in May 2006 (Anti-Phishing Working Group, 2006). Data from market analyst Gartner released June, 2007 showed that phishing attacks have doubled over the last two years. 3.5 million adults remembered revealing sensitive personal or financial information to a phisher, while 2.3 million said that they had lost money because of phishing. The average loss is $1,250 per victim. (Kirk, 2007).

PHISHING :INDIAN PERSPECTIVE

Phishing along with spyware seem to be the biggest challenges that corporate India is facing today but the awareness of these high-risk internet threats is low throughout India for both employees as well as IT managers and is almost nil amongst common internet using individuals. Most organizations have still not assumed the onus of responsibility when it comes to protecting their customers from phishing attacks. Too many of them choose to hide behind the 'fine print' of online lack of answerability. There have been several cases of attacks on genuine websites in India, financial institutions being the main targets and the frequency of these attacks is sure to rise with the rise of internet usage in India. About 74% of IT managers across India reported that their employees have received phishing attacks via e-mail or instant messaging on their office PC. 32% of IT employees in India admitted to have given out their confidential data such as credit card numbers and corporate network passwords as a result of phishing attacks. 34 per cent of IT managers in India claim to be extremely well protected against spyware and phishing attacks. However, despite this confidence, 52 per cent of IT managers stated that their workstations might have been infected by spyware. (India Web@Work survey, 2005).

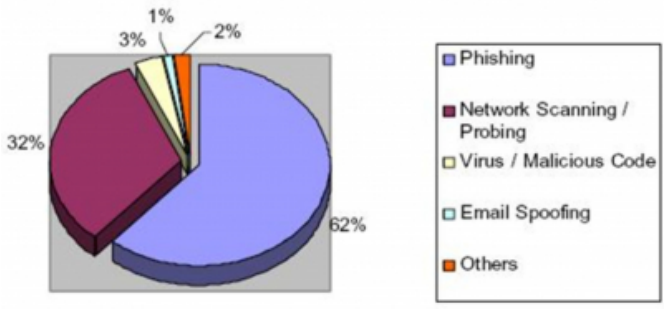
Many experts believe that the risk of cyber attacks is significantly under-detected and under-reported in the United States. These problems of detecting and reporting appear to be far worse in the rest of the world including India. The awareness amongst the internet users in India is

so low that many victims don't even know they've been hit; as a result most of the cases go unreported. The reasons for this are not hard to understand and probably reflect that their citizens are not often victims of cyber-crimes, that it is difficult to find and train (and pay) capable people to collect such information and carry out investigations, and that almost any other form of crime probably has higher priority for the limited law enforcement resources available in the country. (Camp, et al.). Given the proper systems, there would be a substantial increase in the number of cases registered. The law enforcers – the police – need to be educated through training sessions on such technology frauds.

India's relatively unsafe e-security environment is mostly affecting the BPO/ITES industry. The IT Act (2000) needs to crucially define cyber harassment, phishing and cyber stalking to take care of cyber crimes in India. With the Indian IT/BPO exports to reach $60 billion by 2010, such companies need to invest in upgrading security measures for sustaining competitiveness. (Mathur, 2007). Out of the 550 incidents handled by CERT India in 2006 62% were reported to be of phishing Fig. 2. E-Commerce sector topped the list of targets for phishing attacks with 75% share followed by Financial Services which accounted for 24% of the total number of incidents reported in 2006. The number of incidences of phishing has grown substantially over the period of time, In 2004 there were only 4 cases which grew to 101 in 2005 and further elevated to 339 in 2006. (CERT-In Annual Report, 2006).

Figure 2

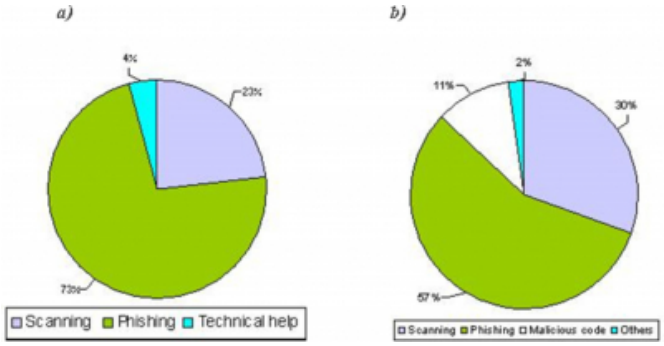
Figure 2: Share of Phishing in incidences of cyber crimes reported to CERT-In in 2006



In March 2007, 47 security incidents were reported to CERT-In from various National / International agencies. 73% of reported incidences were of phishing. In May, 46 security incidents were reported out of which 57% were of phishing registering decrease as compared to March, but, the percentage again rose to 60% in June 2007. (Indian Computer Emergency Response Team, 2007).

Figure 3

Figure 3: a) Share of phishing in incidences of cyber crimes reported in March 2007, b) Share of phishing in incidences of cyber crimes reported in May 2007.



If we look at the world phishing statistics then Asia receives only 8.51% of phishing attacks and India is rated as a quiet country. (AVIRA antivirus report). But, a matter of serious concern is that India is increasingly favored by phishers as a base to host their websites from. A dig-style phishing database from Phishtank showed that 8% of the total world phishing websites are hosted from India (Phishtank, 2006) and this share is increasing day by day. This again emphasizes the need to revise the IT act to include a clear definitions and punishments with regards to phishing and other highly organized cyber crimes.

CONCLUSION

In pursuit of faster growth we probably ignored the important aspect of security and this mistake is cutting our pockets now. Phishing is one of the fastest growing internet crimes, yet most of the Internet users do not have any idea what phishing is, many don't even know the word phishing. With an increasing amount of commerce online, this is extremely worrisome. Although there are many technological solutions that could be employed to protect oneself against phishing attacks, but, easiest and seemingly the best way of combating phishing and other attacks that target individuals through online interactions is increased user awareness. Clearly, a person familiar with phishing and possible intensions of the attacker is less likely to become victim of the attack.

References

1. Anti-Phishing Working Group, Phishing Activity Trends Report (May 2006). http://www.antiphishing.org/reports/apwg_report_May2006.pdf.
2. Anti-Phishing Working Group. Phishing Activity Trends Report (November, 2005).

3. AVIRA antivirus report.
http://www.avira.com/en/threats/section/worldphishing/top/7/index.html.
4. Camp LJ, Goodman S, House CH, Jack WB, Ramer R and Stella M. Chapter 6: Offshoring: Risks and Exposures http://www.acm.org/globalizationreport/chapter6.pdf.
5. CERT-In Annual Report (2006).
http://cert-in.org.in/knowledgebase/annualreport/annualreport06.pdf
6. Emigh, A (2005). Online identity theft: Phishing technology, chokepoints and countermeasures. ITTC Report on Online Identity Theft Technology and Countermeaures; http://www.anti-phishing.org/Phishing-dhs-report.pdf.
7. Gabrilovich E and Gontmakher A. (2002). "The Homograph Attack," Communications of the ACM, 45(2):128.
8. Gartner Inc. (2004). Gartner study finds significant increase in e-mail phishing attacks.
http://www.gartner.com/5 about/press releases/asset 71087 11.jsp.
9. India Web@Work survey (2005). Websense Inc & Dynamic Markets Limited
10. Indian Computer Emergency Response Team.
http://www.cert-in.org.in/knowledgebase/SecurityBulletin/
11. Kirk J. (2007). Phishing Tool Constructs New Sites in Two Seconds.
http://www.pcworld.in/news/index.jsp/artId=5800046
12. Mathur SK (2007). Indian IT industry: a performance analysis and a model for possible adoption MPRA Paper No. 2368, http:// mpra.ub.uni-muenchen.de/ 2368/
13. Phishtank (October 2006). A digg-style phishing database by OpenDNS folks. Phishing states by county of Host.
14. Wetzel R (2005). Tackling Phishing. Buisness communications Review.
http://www.netforecast.com/Articles/RW-Phishing-CR05,02.pdf.

Author Information

Bharat B. Bhagat
Sher-e-Kashmir University of Agricultural Sciences and Technology

Latika Kharb
Research Scholar, Deptt of Computer Sc & Applications, M.D.University