# A Survey: Web based Cyber Crimes and Prevention Techniques

Jheel Somaiya
Dept. of Computer Engineering,
D.J. Sanghvi COE
Vile Parle (W),
Mumbai.

Dhaval Sanghavi
Dept. of Computer
Engineering, D.J. Sanghvi COE
Vile Parle (W),
Mumbai.

Chetashri Bhadane
Assit.Prof. Dept. of
Engineering, D.J. Sanghvi
Vile Parle (W),
Mumbai.

## ABSTRACT

Offences those are committed against an individual or a groupwith a criminal motive to intentionally harm the reputation or cause physical or mental harm to the victim using modern telecommunication networks such as the Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS) are termed as cyber-crimes. Cyber-crime is any illegal activity that uses a computer as its primary means. There are two main categories that define the make-up of cyber-crimes. Firstly viruses, malware, or denial of service attacks that target computer networks or devices. The second category relate to crimes that are facilitated by computer networks or devices like cyber-stalking, fraud, identity-theft, extortion, phishing (spam) and theft of classified information. It is widely known that victims of Internet crimes are often reluctant to report an offence to authorities or in some cases the individual may not even be aware a crime has been committed. Even though facilities for reporting incidents of cyber-crime have improved in recent years many victims remain reluctant to do so due to embarrassment. International cooperation is essential if a good response is to be found against global cyber-crime. No nation can effectively combat the issue alone in an easy way. Many computer based crimes are initiated 'off-shore' and this presents enormous challenges to any nations agencies of law enforcement. It is crucial that agencies from around the world formulate actionable plans to detect, follow, arrest and prosecute criminals of cyber-crime. Computers and the Internet have been a boon to our society; unfortunately criminals now make use of these technologies to detriment our society.

## General Terms

Cybercrime, Cyber space, Cybercrime variants, Prevention Techniques

## Keywords

Cyber Stalking, Hacking, Phishing, Cross Site Scripting, Vulnerability

## 1. INTRODUCTION

The world of Internet today has become a parallel form of life. Public are now capable of doing many things which were unimaginable few years ago. The Internet is becoming a way of life for many people and also a way of living because of growing dependence and reliance of the mankind on these machines. Internet has made the use of website communication, email and a lot of anytime anywhere for the betterment of human kind. Internet, though offers great benefit to society, also present Opportunities for crime using ne and highly sophisticated technology tools. Today websites and emails have become the preferred means of communication. By their very nature, they facilitate almost instant exchange of data, images and variety of material. This includes not only educational informative material but also information that might be not desirable or anti-social. Many common stories featured in the media on computer crime include topics covering hacking to viruses, web-hackers, to internet pedophiles, sometimes accurately portraying events, sometimes misconceiving the role of technology in such activities. Increase in cyber-crime rate has been documented in the news media. The gradual increase in the incidence of criminal activity and the possible emergence of new varieties of criminal activity pose challenges for legal systems.

## 2. CYBER CRIME AND TRADITIONAL CRIME

What we should realize is that those behind these cyber-criminal acts are often involved in traditional crimes such as prostitution, kidnapping, theft, human and drug trafficking, as well as money laundering. These are associated with international organized crime and mob activities. The only difference is that they are now utilizing Internet facilities such as emails, websites and blogs, social networking sites, on-line chat rooms, and electronic bulletin boards as alternative channels to conduct their activities. The highest number of incidents reported to the Cyber999 Help Centre, managed by Cyber Security Malaysia in 2010, falls under the Fraud and Intrusion category at 35 percent for intrusion and intrusion attempts and 27 percent for fraud. This is then followed by spam at 16 percent and malicious codes (malware) at 15 percent. However, in the same period, Cyber Security Malaysia detected 155,809 spam emails, which include

24,644 spams of network and connect rejects as well as 1,377 spams that contain malware. Therefore, it can be said that the total 1,266 spams reported by the public to Cyber999 consist merely 0.8 percent of the total detected spams. This inevitably means that spam represents the largest number of unreported cases. So, a high number of cyber security incidences remain undetected by the user. Perhaps, Internet users do not know if these incidences can be reported or to whom they should report it to. This makes it difficult to catch and convict spammers who are actually criminals using spams to trap their victims.

## 3. CYBER SPACE AND CYBER CRIME

Cyber space is a collective noun for the diverse range of environments that have arisen using the Internet and the various services. The expression crime is defined as an act, which subjects the doer to punishment or any offence against morality, social order or any unjust or shameful act. The "offence" is defined in the Code of Criminal Procedure to mean as an act or omission made punishable by any law for the time being in force. Cyber-crime is a term used to broadly describe criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity and include everything from electronic cracking to denial of service attacks

## 4. CYBER CRIME VARIANTS

There are a good number of cyber-crime variants. A few varieties are discussed for the purpose of completion. This article is not intended to expose all the variants. The readers are directed to other resources.

### 4.1 Cyber Stalking

Cyber stalking is use of the Internet or other electronic means to stalk someone. This term is used interchangeably with online harassment and online abuse. Stalking generally involves harassing or threatening behavior that an individual engages in repeatedly, such as following a person, place of business or appearing at a person's home, making harassing phone calls, vandalizing a person's property.

### 4.2 Hacking

"Hacking" is a crime, which entails cracking systems and gaining unauthorized access to the data stored in them. Hacking had witnessed a 37 % rise this year.

### 4.3 Phishing

Phishing is just one of the many frauds on the Internet, trying to bluff people into parting with their money. Phishing refers to the unsolicited emails by customers of financial institutions, requesting them to enter their username, password or other personal information to access their account for some reason. Customers are directed to a fraudulent replica of the original institution's website when they click on the links on the email to enter their information, and so they are unaware that the fraud has occurred. The fraudster then has access to the customer's online bank account and to the funds contained in that account. F-Secure Corporation's summary of 'data security' threats during the first half of 2007 has revealed that the study found the banking industry as soft target for phishing scams in India [The Business line Monday July 23 2007]. Phishing is the criminal practice of using social engineering and Voice over IP (VoIP) to gain access to private .personal and financial Information from the public for the purpose of financial reward. The term is a combination of "voice" and phishing. Phishing exploits the public's trust in landline telephone services, which have traditionally terminated in physical locations which are known to the telephone company, and associated with a bill-payer. Phishing is typically used to steal credit card numbers or other information used in identity theft schemes from individuals

### 4.4 Cross Site Scripting

Cross-site scripting (XSS) is a type of computer security vulnerability typically found in web applications which allow code injection by malicious web users into the web pages viewed by other users. Examples are client-side scripts and HTML codes.

### 4.5 Vulnerability

The Open-Source Vulnerability Database (OSVDB) project maintains a master list of computer security vulnerabilities, freely available for use by security professionals and projects around the world. Vulnerability information is critical for the protection of information systems everywhere: in enterprises and other organizations, on private networks and on the public Internet.

## 5. INDIAN CRIME SCENE

The major cyber-crimes reported, in India, are denial of services, defacement of websites, SPAM, computer virus and worms, pornography, cyber-squatting, cyber stalking and phishing. [l] Given the fact that nearly $ 120 million worth of mobiles are being lost or stolen in the country every year, the users have to protect information, contact details and telephone numbers as these could be misused. India has to go a long way in protecting the vital information. Symantec shares the numbers from its first systematic survey carried out on the Indian Net Security scene: The country has the highest ratio in the world (76 per cent) of outgoing spam or junk mail, to legitimate e-mail traffic. India's home PC owners are the most targeted sector of its 37.7 million Internet users: Over 86% of all attacks, mostly via 'bots' were aimed at lay surfers with Mumbai and Delhi emerging as the top two cities for such vulnerability.

### 5.1 Phishing Case in India

Phishing attacks were more popular among Indian users due to rising Internet penetration and growing online transactions. India has now joined the dubious list of the world's top 15 countries hosting "phishing" sites which aims at stealing confidential information such as passwords and credit card de- tails. [The Hindu Sunday Nov 26 2006] A non-resident Malayali, had an account in a nationalized bank in Adoor, lost $ 10,000 when the bank authorities heeded a fake e-mail request to transfer the amount to an Account in Ghana. In Mangalapuram, a person transferred a large sum of money as "processing charge” to a foreign bank account after he received an e-mail, which said he had won a lottery LKerala: The Hindu Monday Oct 30 2006] Reports of phishing targeted at customers of banks. Appear to be on the rise. Websense Security Labs, in a statement released recently, said it had received reports of such attacks from customers of AXIS Bank. The Economic Of-fences Wing (EOW), Crime Branch, Delhi Police, unearthed a major phishing scam involving fake emails and websites of UT1 Bank, An analysis of the accounts of the four arrested Nigerian nationals indicated financial transactions of over Rs 1 crore in an eight-month period till December 2006. Investigations revealed that the scam is multi-layered with pan-India and international characteristics The Lab went on to say that it found a mal ware in the Web site of Syndicate Bank. The users through a spoofed e mail were asked to renew certain services and claiming that failure to do so would result in suspension or deletion of the account. The e-mail provided an l ink to a malicious site that attempted to capture the personal and account information. [The Hindu, Monday August 20 2007]. Phishing emails have increased by approximately twenty five percent over the last year but are harder to detect as they increasingly trick unsuspecting people with ordinary scenarios instead of improbable ones such as sudden cash windfalls. It has been six months since the phishing attack on ICICI bank customers became public, and during that period, two more such attacks were reported on customers of financial institutions in India, one of UTI Bank and the other. State Bank of lndia. [5-Jan 17-theHindu] RSA's 24/7 Anti-Fraud Command Centre f AFCC) has just uncovered a ‘Universal man-in-the middle Phishing Kit' in online forums which helps phishers quickly create the fraudulent websites, often borrowing code from the original site. [The Hindu Wednesday, Jan 17 2007]

## 5.2 Cyber Cafes and Emails

Cyber cafes have emerged as hot spots for cybercrimes. Even terrorists prefer the anonymity of a cyber cafe to communicate with each other. The mushrooming of cyber cafes in the city, which provide the secrecy through cabins constructed for users, has also made the porn literature easily accessible to the people visiting them. (Chandigarh Tribune Monday May 28 2001] A 23- year-old person from Tiruchi was arrested by the City Cyber Crime police on Thursday on charges of sending an e-mail threat to the Chief Minister and his family. [The Hindu Friday Aug 10 2007] In another case, the police team investigating the e-mail threat on the lives of the President and the Prime Minister has prepared a sketch of the suspect, who had sent the email from a cyber cafe in the city. [The Hindu, Sunday Ocober 29 2006]. The Case of The State of Tamil Nadu Vs Suhas Katti is notable for the fact that the conviction was achieved successfully. The case related to posting of obscene and annoying message about a divorcee woman in the yahoo message group. E-Mails were also send to the victim for information by the accused through a false e-mail account opened by him in the name of the victim. The message resulted in annoying phone calls to the lady. A travel agent was arrested for allegedly sending a threatening mail to blow up the National and Bombay stock exchanges in Kolkata [Express India.com Sun 28 Oct 2007].

## 5.3 Phishing

A tenth standard boy from Bangalore got into trouble when a girl much older than him started stalking him. She pasted I Love You' slips on his gate and called his On reviewing his Orkut profile, it was realized that he had accepted chat invites from more than 20 people; only two of who were his real-life friends. [The Hindu Tuesday, May 01, 2007]

# 6. PREVENTION TECHNIQUES

## 6.1 Cyber Stalking

Do not share personal information in public spaces anywhere online, or with strangers, including in e-mail or chat rooms. Do not use your real name as your screen name or user ID. Pick a name that is gender and age neutral. And do not post personal information as part of any user profile. Be extremely cautious about meeting online acquaintances in person. If you choose to meet, do so in some public place and take along a friend or a relative. Make sure that your ISP and Internet Relay Chat (IRC) network have an acceptable use policy that prohibits cyber stalking. If your network provider fails to respond to your complaints, then switch to a provider that is more responsive to user complaints and values its users. If a situation places you in fear or threat, contact a local law enforcement agency.

## 6.2 Hacking

The computer you use to manage your website should be highly secured. If hackers access your computer, they have an easy access to your website and data. Your computer needs the best quality antivirus software available that detects a virus the moment it is received. Web server software needs to be kept up to date. According to Matt Cutts, the best preventive method you can take is to patched. Use strong passwords and change them often. This sounds very simple, but is an area many people tend to neglect. A weak password of only four characters can be hacked in less than one second. Secure your email address by using software that prevents the spammer program from reading the email address. Create proper access permissions to your website by making it read- only. Make sure you are using the latest versions of all third party scripts by carefully choosing third party scripts that are trustworthy. Some free scripts may compromise the security of your website. The latest version is always the safest. Make back-up copies of all your website files, no matter how many protections you have in place. Even after this it is still possible for your website to be hacked. If you regularly back-up your website, you will at least be able to restore it quickly.

## 6.3 Phishing

If you receive an email from your bank informing you that it suspects an unauthorized transaction on your bank account and asking you to click on a link to verify your identity information, then do not click on the link as it may contain viruses and spyware. If you receive an e-mail from your organization asking you to confirm your password and share your personal data by entering into secure website don’t do that because it can be a type of phishing attack, where attacker wants your personal data by making himself as a trusted person of an organization. Despite of your precautions if you have been phished and you have given your personal information to someone who is masquerading as your online payment service, ISP, bank or even a government agency then take the following steps-Keep reviewing the copy of your credit report periodically to look for any new account activity. Contact immediately to the concerned organization and file a report of cyber-crime to the police as soon as possible.

## 6.4 Cross Site Scripting

The following list states the general approaches to prevent cross-site scripting attacks: Encode output based on the input parameter set. Filter input parameter set for special characters. Filter output based on input parameter set for special characters. When a user encodes or filters, he must specify a character set for his Web pages to ensure that his filter is checking for the appropriate special characters. The data inserted into his Web pages should filter out byte sequences that are considered special characters based on the specific character set. A popular character set is ISO 8859-1, which was the default set in early versions of HTTP and HTML. The user must take into account issues of localization when he changes these parameters.

## 6.5 Vulnerability

For amateurs, as a best practice, certain functionality should be made accessible via a VPN. All admin functionality should be remapped onto internal IPs, which can then be accessed only by certain IPs over a VPN. Programmers frequently rely too much on frameworks (like the .NET validate-request feature) to defend against dangerous inputs, or use application firewalls based on signatures that work by blacklisting the various attack vectors published by hackers in SQL injection cheat sheets or cross-site scripting (XSS). This approach is flawed, as custom attacks can bypass the protection afforded by .NET and simple blacklists. The best approach for addressing such security vulnerabilities in Web applications is to validate correctly the input while writing the software, or update the code after the app has been deployed with the help of a pen tester or programmer. Making sure that programs and users that run as users have the minimum number of rights necessary to do their jobs, and no more, is most importance for authentication and access control. It is still common for default error pages to be left in place; this might allow the SQL database structure to be easily enumerated. More seriously is that such errors are likely to be captured by search engine crawls or Google, which hacker groups can then use to discover the servers that are potentially vulnerable for attack. Default accounts with usernames such as ‘administrator’, ‘admin’, 'anonymous' or 'test' are rarely removed or renamed, which makes things very easy for attackers, as only the password needs to be brute-forced. Broken access control mechanisms, which allow users to modify or read other user’s documents, can be achieved by knowing the document ID, or by guessing other document names. In the same manner, gaining access to admin programs by brute-forcing program names, within directories found to exist, for example /admin/. If an attacker takes over an account, he can then message other users from the account, or perform other unnecessary actions, like forwarding messages to the compromised user's mailing list or changing their passwords.

## 7. ANTICYBER CRIME INITIATIVES

In a first of its kind initiative in India to tackle cyber-crime, police have taken the initiative to keep an electronic eye on the users of the various cyber cafes spread over the city. The Kerala State IT Mission has launched a Web portal and a call center to tackle cyber-crime. The Central Bureau of Investigation (CBI) and the Mumbai police have recommended issuance of licenses to cyber café owners. Many countries, including India, have established Computer Emergency Response Teams (CERTs) with an objective to coordinate and respond during major security incidents/events. These organizations identify and ad-dress existing and potential threats and vulnerabilities in the system and coordinate with stakeholders to address these threats. Policy initiatives on cyber-crime are as yet lethargic because of a general sense that it is nothing more than juvenile hackers out to have fun or impress someone. Prateek Bhargava, cyber law expert says, "There is high potential for damage to national security through cyber-attacks. The internet is a means for money laundering and funding terrorist attacks in an proper manner. In the words of Pavan Duggal, Supreme Court Lawyer, “Cyber-crime is omnipresent and although cyber-crime cells have been set up in major cities, most cases remain unreported due to lack of awareness."

## 8. CONCLUSION

Net surfing by youngsters lures them into dangerous do- main. The need for a conscious effort to checkmate the undesirable fallout of youngsters accessing and using the Internet is of concern. The print media has a duty unwary parents and youngsters about the dangers inherent in treading dangerous areas in the cyber-world. Cyber Space Security Management has already become an important component of National Security Management, Military related Scientific Security Management and Intelligence Management all over the world. Intelligence operations and covert actions will increasingly become cyber-based. It is of great importance that our intelligence agencies gear themselves up to this new threat. It is, thus, necessary to put in place a 'National Cyber Space Security Management Policy' to define the tasks, specify responsibilities of individual agencies with an integrated architecture. It is a fact that terrorists have been using the Internet to communicate, extort, intimidate, raise funds and coordinate operations. Hostile states have highly developed capabilities to wage cyber wars. They have the capability to paralyze large parts of communication net- works, cause financial meltdown and unrest. The degree of our preparedness in the face of all these potential threats, does leaves much to be desired. The Government should also take note of this slow but worrying development and put in place a proper mechanism to curb the misuse.

## 9. REFERENCES

[1] Cordy E, “The legal regulation of e-commerce transact-tions”, Journal of American Academy of Business, vol. 2, no. 2, pp. 400-407, 2009.

[2] Cyber Crime Today & Tomorrow, Thiru Dayanithi Maran.

[3] Geer D, “Security technologies go phishing”, Computer, vol. 38, no. 6, pp. 18-21, 2010.

[4] MacInnes I, Musgrave D, and Laska J, “Electronic commerce fraud: towards an understanding of the phenomenon”, Proceedings of the 38th Annual Hawaii International Conference, 2011.

[5] McCrohan K, “Facing the threats to e-commerce”, The Journal of Business & Industrial Marketing, vol. 18, no. 2/3, pp. 133-145, 2011.

[6] McCusker R, “E-Commerce, Business and Crime: Inextricably Linked, Diametrically Opposed”, The Company Lawyer, vol. 23, no. 1, pp. 3-8, 2012.

[7] Sukha N, “Hacking and cybercrime”, Proceedings of the 1st Annual Conference on Information Security Curriculum Development-ACM, pp. 128-132, 2012.