PHISHING ATTACKS AND CYBER CRIMES : AN CURRENT VIEW

KISHAN LAL[1]
JAGPAL SINGH[2]
DR. ANIL KUMAR SHROTRIYA[3]

[1]Research Scholar- (Computer Science)
Research Department, JJT University
Jhunjhunu, Rajasthan (India)
E-mail: godara123456@gmail.com

[2]Research Scholar- (Computer Science)
, Research Department, JJT University
Jhunjhunu, Rajasthan (India)
E-mail: jagpals@compucom.co.in

[3]Professor, (Department of Physics)
Shri P.S.B. Govt. P.G. College, Shahpura
Distt.- Bhilwara, Rajasthan (India)
E-mail: anilshrotriya@rediffmail.com

ABSTRACT

This overview gives the basic introduction of cyber laws and phishing attacks, defines the terms used in the industry and research field, outlines the detail of cyber laws and architecture of prevention from phishing. It provides a brief summary of anti-phishing and provides a good foundation for understanding the effects and prevention of phishing.

Keywords: Law, Cyber, Architecture, *Phishing, and Prevention.*

1. WHAT IS CYBER LAW?

Cyber crime is the latest and perhaps the most complicated problem in the cyber world. Cyber crime is now amongst the most important revenue sectors for global organized crime. Any criminal activity that uses a computer either as an instrumentality, target or a means for perpetuating further crimes comes within the ambit of cyber crime. 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.

A generalized definition of cyber crime may be " *unlawful acts wherein the computer is either a tool or target or both".* The computer may be used as a tool in the following kinds of activity- financial crimes, sale of illegal articles, pornography, online gambling, intellectual property crime, e-mail spoofing, forgery, cyber defamation, cyber stalking. The computer may however be target for unlawful acts in the following cases- unauthorized access to computer/ computer system/ computer networks, theft of information contained in the electronic form, e-mail bombing, data didling, salami attacks, logic bombs, Trojan attacks, internet time thefts, web jacking, theft of computer system, physically damaging the computer system.

Cyber Law is the law governing cyber space. Cyber space is a very wide term and includes computers, networks, software, data storage devices, the Internet, websites, emails and even electronic devices such as cell phones, ATM machines etc. Law encompasses the rules that have been approved by the government, and which are in force over a certain territory, and which must be obeyed by all persons on that territory.

Violation of these rules could lead to government action such as imprisonment or fine or an order to pay compensation.

Cyber law encompasses laws relating to:

1. Cyber Crimes
2. Electronic and Digital Signatures
3. Intellectual Property
4. Data Protection and Privacy

Cyber crimes are unlawful acts where the computer is used either as a tool or a target or both. The enormous growth in electronic commerce and online share trading has led to a phenomenal spurt in incidents of cyber crime. Electronic signatures are used to authenticate electronic records. Digital signatures are one type of electronic signature.

1.1 REQUIREMENT FOR CYBER LAW

1. Cyberspace is an **intangible** dimension that is impossible to govern and regulate using conventional law.
2. Cyberspace has complete **disrespect for jurisdictional boundaries**. A person in India could break into a bank's electronic vault hosted on a computer in USA and transfer millions of Rupees to another bank in Switzerland, all within minutes. All he would need is a laptop computer and a cell phone.
3. Cyberspace handles **gigantic traffic volumes every second**. Billions of emails are crisscrossing the globe even as we read this, millions of websites are being accessed every minute and billions of dollars are electronically transferred around the world by banks every day.
4. Cyberspace is absolutely **open to participation by all**. A ten year- old in Bhutan can have a live chat session with an eight year- old in Bali without any regard for the distance or the anonymity between them.
5. Cyberspace offers **enormous potential for anonymity** to its members. Readily available encryption software and steganographic tools that seamlessly hide information within image and sound files ensure the confidentiality of information exchanged between cyber-citizens.
6. Cyberspace offers never-seen-before **economic efficiency**. Billions of dollars worth of software can be traded over the Internet without the need for any government licenses, shipping and handling charges and without paying any customs duty.
7. A software source code worth crores of rupees or a movie can be **pirated across the globe** within hours of their release.

2. TYPES OF CYBER CRIME

Categories of Cyber crimes

Cyber crimes can be basically divided into 3 major categories being Cyber crimes against persons, property and Government.

1.**Cyber crimes against persons**

Cyber crimes committed against persons include various crimes like transmission of child-pornography, harassment of any one with the use of a computer such as e-mail, and cyber-stalking. The trafficking, distribution, posting, and dissemination of obscene material including pornography, indecent exposure, and child pornography, constitutes one of the most important Cyber crimes known today.

2.**Cyber Crimes against property**

The second category of Cyber crimes is that of Cyber crimes against all forms of property. These crimes include unauthorized computer trespassing through cyberspace, computer vandalism, transmission of harmful programs, and unauthorized possession of computerized information.

3.**Cyber Crimes against Government**

The third category of Cyber crimes relate to Cyber crimes against Government. Cyber Terrorism is one distinct kind of crime in this category. The growth of Internet has shown that the medium of Cyberspace is being used by individuals and groups to threaten the international governments as also to terrorism the

citizens of a country. This crime manifests itself into terrorism when an individual "cracks" into a government or military maintained website.

1. **Hacking**- Hacking in simple terms means illegal intrusion into a computer system without the permission of the computer owner/user. Hacking is a crime, which entails cracking systems and gaining unauthorized access to the data stored in them.

2. **Denial of Service Attack**- This is an act by the criminal , who floods the bandwidth of the victim's network or fills his e-mail box with spam mail depriving him of the services he is entitled to access or provide

3. **Virus Dissemination**- Malicious software that attaches it self to other software. (virus, worms , Trojan Horse , Time Bomb , Logic Bomb , Rabbit and Bacterium are the malicious software)

4. **Software Piracy**-
• Theft of software through the illegal copying of genuine programs or the counterfeiting and distribution of products intended to pass for the original .
• Retail revenue losses worldwide are ever increasing due to this crime
• Can be done in various ways- End user copying , Hard disk loading , Counterfeiting , Illegal downloads from the internet etc .

5. **Pornography**- Pornography is the first consistently successful e-commerce product.
• Deceptive marketing tactics and mouse trapping technologies Pornography encourage customers to access their websites.
• Anybody including children can log on to the internet and access websites with pornographic contents with a click of a mouse.
• Publishing, transmitting any material in electronic form which is lascivious or appeals to the prurient interest is an offence under the provisions of section 67 of I.T. Act -2000.

6. **IRC Crime**- Internet Relay Chat (IRC) servers have chat rooms in which people from anywhere the world can come together and chat with each other
• Criminals use it for meeting coconspirators.
• Hackers use it for discussing their exploits / sharing the techniques
• Pedophiles use chat rooms to allure small children
• Cyber Stalking - In order to harass a woman her telephone number is given to others as if she wants to befriend males

7. **Credit Card Fraud**- You simply have to type credit card number into www page o f the vendor for online transaction If electronic transactions are not secured the credit card numbers can be stolen by the hackers who can misuse th s card by impersonating the credit card owner

8. **Net Extortion**- Copying the company's conf dential data in order to extort said company for huge amount .

9. **Phishing**- It is technique of pulling out confidential information from the bank/financial institutional account holders by deceptive means. Phishing is just one of the many frauds on the Internet, trying to fool people into parting with their money. Phishing refers to the receipt of 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.

10. **Spoofing**- Getting one computer on a network to pretend to have the identity o f another computer , usually one with special access privileges, so as to obtain access to the other computers on the network .

11. **Cyber Talking**- The Criminal follows the victim by sending emails , entering the chat rooms frequently . 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, appearing at a person's home or place of business, making harassing phone calls, leaving written messages or objects, or vandalizing a person's property.

12. **Cyber Defamation**- The Criminal sends emails containing defamatory matters to all concerned of the victim or post the defamatory matters on a website . (disgruntled employee may do this against boss , ex-boys friend against g rl , divorced husband against wife etc)

13. **Threatening**- The Criminal sends threatening email or comes in contact in chat rooms with victim . (Any one disgruntled may do this against boss , friend or official)

14. **Sale of Narcotics**
• Sale & Purchase through net .
• There are web site which offer sale and shipment o f contrabands drugs .
• They may use the techniques of stenography for hiding the messages

15. 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 of such code include HTML code and client-side scripts. An exploited cross-site scripting vulnerability can be used by attackers to bypass access controls.

2.1 PREVENTION FOR INDIVIDUALS

Children:- Children should not give out identifying information such as Name, Home address, School Name or Telephone Number in a chat room. They should not give photographs to anyone on the Net without first checking or informing parents guardians. They should not respond to messages, which are suggestive, obscene, belligerent or threatening, and not to arrange a face-to –face meeting without telling parents or guardians. They should remember that people online might not be who they seem.

Parents: - Parent should use content filtering software on PC to protect children from pornography, gambling, hate speech, drugs and alcohol. There is also software to establish time controls for use of limpets and allowing parents to see which site item children have visited. Use this software to keep track of the type of activities of children.

General information: - Don't delete harmful communications (emails, chats etc). They will provide vital information about system and address of the person behind these.

- Be extremely careful about how you share personal information about yourself online.
- Choose your chatting nickname carefully so as others.
- Do not share personal information in public space online; do not give it to strangers.
- Be extremely cautious about meeting online introduced person. If you choose to meet, do so in a public place along with a friend.
- Try not to panic.
- If you feel any immediate physical danger contact your local police.
- Avoid getting into huge arguments online during chat and discussions with other users.
- Remember that all other Internet users are strangers; you do not know who you are chatting with. So be careful.
- If a situation online becomes hostile, log off and if a situation places you in fear, contact local police.
- Save all communications for evidence. Do not edit it in any way. Also, keep a record of your contacts and inform Law Enforcement Officials.

2.2 PREVENTION FOR GROUPS

Physical Security: Physical security is most sensitive component, as prevention from cyber crime Computer network should be protected from the access of unauthorized persons.

Access Control: Access Control system is generally implemented using firewalls, which provide a centralized point from which to permit or allow access. Firewalls allow only authorized communications between the internal and external network.

Password: Proof of identity is an essential component to identify intruder. The use of passwords in the most common security for network system including servers, routers and firewalls. Mostly all the systems are programmed to ask for username and password for access to computer system. This provides the verification of user. Password should be charged with regular interval of time and it should be alpha numeric and should be difficult to judge.

Finding the holes in network: System managers should track down the holes before the intruders do. Many networking product manufactures are not particularly aware with the information about security holes in their products. So organization should work hard to discover security holes, bugs and weaknesses and report their findings as they are confirmed.

Using intrusion alert program: As it is important to identify and close existing security holes, you also need to put some watchdogs into service. There are some intrusion programs, which identify suspicious activity and report so that necessary action is taken. They need to be operating constantly so that all unusual behavior on network is caught immediately.

Using encryption: - Encryption is able to transform data into a form that makes it almost impossible to read it without the right key. This key is used to allow controlled access to the information to selected people. The information can be passed on to any one but only the people with the right key are able to see the information. Encryption allows sending confidential documents by E-mail or save confidential information on laptop computers without having to fear that if someone steals it the data will become public. With the right encryption/decryption software installed, it will hook up to mail program and encrypt/decrypt messages automatically without user interaction.

2.3 PREVENTION STEPS

It is always better to take certain precaution while operating the internet. A internet users should keep in mind the following things-

1. To prevent cyber stalking avoid disclosing any information pertaining to oneself. This is as good as disclosing your identity to strangers in public place.
2. Always avoid sending any photograph online particularly to strangers and chat friends as there have been incidents of misuse of the photographs.
3. Always use latest and up date anti virus software to guard against virus attacks.
4. Always keep back up volumes so that one may not suffer data loss in case of virus contamination
5. Never send your credit card number to any site that is not secured, to guard against frauds.
6. Always keep a watch on the sites that your children are accessing to prevent any kind of harassment or depravation in children.
7. It is better to use a security programme that gives control over the cookies and send information back to the site as leaving the cookies unguarded might prove fatal.
8. Web site owners should watch traffic and check any irregularity on the site. Putting host-based intrusion detection devices on servers may do this.
9. Use of firewalls may be beneficial.
10. Web servers running public sites must be physically separate protected from internal corporate network.

2.4 DETECTION

Cyber crime is the latest and perhaps the most specialized and dynamic field in cyber laws. Some of the Cyber Crimes like network Intrusion are difficult to detect and investigation even though most of crimes against individual like cyber stalking, cyber defamation, cyber pornography can be detected and investigated through following steps:

(1) Give command to computer to show full header of mail.

(2) In full header find out the IP number and time of delivery of number and this IP number always different for every mail. From this IP number we can know who was the Internet service provider for that system from which the mail had come.

(3) After opening the website of any of above mentioned search engine, feed the IP number and after some time name of ISP can be obtained.

(4) After getting the name of ISP we can get the information about the sender from the ISP by giving them the IP number, date and time of sender.

(6) ISP will provide the address and phone number of the system, which was used to send the mail with bad intention.

After Knowing the address and phone number criminal can be apprehended by using conventional police methods.

3. Phishing

In *phishing*, an automated form of social engineering, criminals use the Internet to fraudulently extract sensitive information from businesses and individuals, often by impersonating legitimate web sites.

The term *phishing* is a general term for the creation and use by criminals of e-mails and websites – designed to look like they come from well-known, legitimate and trusted businesses, financial institutions and government agencies – in an attempt to gather personal, financial and sensitive information.

Phishing is committed so that the criminal may obtain sensitive and valuable information about a consumer, usually with the goal of fraudulently obtaining access to the consumer's bank or other financial accounts. Phishing is a way of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication.

3.1 Phishing Techniques from Attacker's Point of View

(1) Simple Phishing
In this phishing attack, attacker will be creating a fake login page similar to the original login page on his server/domain. Once the phishing page is ready. Attacker will convince victim to login using that fake login page and when victim will submit username/password in that fake login page that information will be sent to attacker and victim will be redirected to the original sites login page. Now again victim will have to enter username/password to login in that site and this can make victim suspicious, and victim may identify that there was a trap.

(2) Simple Phishing
In simple phishing attack, attacker will be creating a fake login page similar to the original login page on his server/domain. Once the phishing page is ready. Attacker will convince victim to login using that fake login page and when victim will submit username/password in that fake login page that information will be sent to attacker and victim will be logged into original site. This is done by the attacker to make the attack more stealth and attackers use javascript on their phishing pages which makes the user login into the original site without asking the victim to re-enter the username and password.

(3) Advanced Phishing
In Advanced phishing attack, attacker will be creating a fake login page similar to the original login page on his server/domain. Once the phishing page is ready Attacker will convince victim to login using that fake login page and when victim will submit username/password in that fake login page , that information will further be verified by the server side scripting if the username/password are accurate or wrong and in case details entered by victim are wrong then victim will be again redirected to phishing page and if the details entered by the victim are correct then that information will be sent to attacker and victim w will be logged into original site.

(4) Implementing Ajax keylogger on phishing page
In this Attack, Attacker uses Ajax keylogger on the phishing page. Attackers use AJAX keylogger on their phishing page which saves the keys on the server as user types them and even if the victim don't submit them but just type them still that information is trapped by the attacker and can be further misused.

(5) DNS Poisoning aided Phishing
In this attack, attacker poison the dns of the victim and whenever victim makes a request to the dns victim is given IP address of the Attacker's server where phishing page is hosted, So even if the victim has entered the right Domain name but still victim lands up on the phishing page and the attacker is able to steal the information of the victim. Now in this kind of attack Attacker doesn't even gives a chance to the victim to be suspicious.

The flow of information in a phishing attack is:

1. A deceptive message is sent from the phisher to the user.
2. A user provides confidential information to a phishing server.
3. The phisher obtains the confidential information from the server.
4. The confidential information is used to impersonate the user.
5. The phisher obtains illicit monetary gain.

3.2 Preventing a phishing attack before it begins

Before steps 1-5 above, a phisher must set up a domain to receive phishing data. Pre-emptive domain registration may reduce the availability of deceptively named domains. Additionally, proposals have been made to institute a “holding period” for new domain registrations during which trademark holders could object to a new registration before it was granted. This might help with the problem of deceptively named domains, but would not address the ability of phishers to impersonate sites. As email authentication technologies become more widespread, email authentication could become a valuable preventive measure by preventing forged or misleading email return addresses.

3.3 Detecting a phishing attack

Many different technologies may be employed to detect a phishing attack, including:
• Providing a spoof-reporting email address that customers may send spoof emails to. This may both provide feedback to customers on whether communications are legitimate, and provide warning that an attack is underway.
• Monitoring “bounced” email messages. Many phishers email bulk lists that include nonexistent email addresses, using return addresses belonging to the targeted institution.
• Monitoring call volumes and the nature of questions to customer service.
• Monitoring account activity for anomalous activity such as unusual volumes of logins, password modification, transfers, withdrawals, etc.
• Monitoring the use of images containing an institution’s corporate logos and artwork. Phishers will often use the target corporation to host artwork that is used to deceive customers. This may be detected by a web server via a blank or anomalous “referrer” for the image.
• Establishing “honeypots” and monitoring for email purporting to be from the institution.

3.4 Preventing the delivery of phishing messages

Once a phishing attack is underway, the first opportunity to prevent a phishing attack is to prevent a phishing message from ever reaching a user.

(1) Filtering

Email filters intended to combat spam are often effective in combating phishing as well. Signature-based anti-spam filters may be configured to identify specific known phishing messages and prevent them from reaching a user. Statistical or heuristic anti-spam filters may be partially effective against phishing, but to the extent that a phishing message resembles a legitimate message, there is a danger of erroneously blocking legitimate email if the filter is configured to be sufficiently sensitive to identify phishing email. Phishers depend on being able to make their messages visually appear to be from a trusted sender. One possible countermeasure is to detect unauthorized imagery in emails.

(2) Authentication

Message authentication techniques such as Sender-ID have considerable promise for anti-phishing applications. Sender-ID prevents return address forgery by checking DNS records to determine whether the IP address of a transmitting mail transfer agent is authorized to send a message from the sender's domain. Yahoo! Domain Keys provides similar authentication, using a domain-level cryptographic signature that can be verified through DNS records. Some form of lightweight message authentication may be very valuable in the future in combating phishing. For the potential value to be realized, Sender-ID or a similar technology must become sufficiently widespread that invalid messages can be summarily deleted or otherwise treated prejudicially, and security issues surrounding the use of mail forwarders need to be resolved.

3.5 Defence from users point of view

1) Verify the URL

Before entering any information on the page, make sure that URL on the top of the browser is correct even if you find the look and feel of the page is quite similar to the real login page but make sure to verify that the URL on the top of the browser belongs to the right domain name.

(2) Verify the SSL Certificate

Make sure to verify the SSL Certificate over the domain is there and do belongs to the right Certifying Authority. For example login page of orkut have a ssl certificate of thawte. You can also check the "Lock" icon There is a de facto standard among web browsers to display a "lock" icon somewhere in the window of the browser (NOT in the web page display area!) For example, Microsoft Internet Explorer displays the lock icon in the lower-right of the browser window and As another example, Mozilla's FireFox Web Browser displays the lock icon in the lower-left corner.

(3) Inbult phishing protection in web browsers

Many web browser and added plug-ins today provide you with the security feature which identifies the phishing link and warns you when you visit those links. This security feature is only functional on those links which have been reported by some other user. For example, in case of Mozilla Firefox, Firefox 3 or later contains built-in Phishing and Malware Protection to help keep you safe online.

(4) Internet Security Programs

Many anti-viruses today have phishing protection and works in the similar way as explained above. For example, in case of Norton, Norton Internet Security 2010 Blocks phishing websites and authenticates trusted sites

(5) Password managers can be used.

You can further use various password managers that are available as password manager will only work on the real websites and not on the phishing websites. For example, in case of passpet, Passpet have Convenient Password Management and Phishing Protection

(6) Verifying the IP address of the host
In case you you are suspicious about a page but the URL seems to be correct then you should verify the IP address of that domain , you may be a victim of DNS poisoning. These were the few security measures , by which you can protect yourself from becoming a victim of phishing.

8. CONCLUSION

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. The risks of cyber crime are very real and too ominous to be ignored. At the very least, every company must conduct a professional analysis of their cyber security against cyber crime, engage in a prophylactic plan to minimize the liability; ensure against losses to the greatest extent possible due to cyber crime and implement and promote a well-thought out cyber policy, including crisis management in the event of a worst case scenario. It is not possible to eliminate cyber crime completely from the cyber space. It is quite possible to check them and implements possible preventions by which we can minimize the damages, made by cyber criminals. Previous records are the witness that no legislation has succeeded in totally eliminating crime from the cyber space. The only possible step is to make people aware of their rights and duties and further making the application of the laws more stringent to check crime.

REFERENCES:

[1]. http://www.asianlaws.org/library/cyber-laws/intro-indian-cyber-law.pdf
[2]. http://www.cybercellmumbai.com/files/Types%20of%20cyber%20crime.pdf
[3]. http://www.cidap.gov.in/documents/Cyber%20Crime.pdf
[4]. Phishing Cutting the Identity Theft Line, Rachael Lininger and Russell Dean Vines, Wiley Publishing, Inc. 2005
[5]. http://sparrow.ece.cmu.edu/group/pub/parno_kuo_perrig_phoolproof.pdf
[6]. http://www.justice.gov/opa/report_on_phishing.pdf
[7]. http://www.antiphishing.org/reports/phishing-sfectf-report.pdf
[8].http://www.deloitte.com/assets/Dcom-UnitedStates/Local%20Assets/Documents/AERS/us_aers_ Deloitte%20Cyber%20Crime%20POV%20Jan252010.pdf
[9]. http://www.naavi.org/pati/pati_cybercrimes_dec03.htm
[10]. http://www.gcl.in/downloads/bm_cybercrime.pdf