# Cyber Crimes and Phishing Attacks

Shreya Suman, Neha Srivastava, Renu Pandit

Dronacharya College of Engineering
*Email:nehasrivastava616@gmail.com*

***Abstract*** - This overview gives the basic introduction of cyber laws and phishing attacks, defines the terms used in the industry and research field, outline 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.*

*****

## I. INTRODUCTION

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 organised crime. Any criminal activity that uses a computer either as an instrumentality, target or as a means for perpetuating further crimes comes within the ambit of cyber crime. Cyber crime is a term widely used to describe criminal activity in which computer 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 generalised 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- unauthorised access to computer/ computer system/ computer networks, theft of information contained in the electronic form, e-mail bombing, data didling, salami attacks, logic bombs, Torjan 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 the 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.

## II. 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 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.

6. A software source code worth crores of rupees or a movie can be pirated across the globe within hours of their release.

## III. TYPES OF CYBER CRIME

**Categories of cyber crime**

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

**Cyber Crime against persons**

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

**Cyber Crimes against property**

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

**Cyber Crime 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. Types of cyber crimes are:

1. Hacking
2. Denial of Service Attack
3. Virus Dissemination
4. Software Piracy
5. Pornography
6. IRC Crime
7. Credit Card Fraud
8. Net Extortion
9. Phishing
10. Spoofing
11. Cyber Talking
12. Cyber Defamation
13. Threatening
14. Sale of Narcotics

***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 update antivirus software to guard against virus attacks.
4. Always keep back up volumes so that one way 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.

## IV. 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.

It is a 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.

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.

The flow of information in a phishing attack is:

1. A descriptive 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.

## V. PREVENTING A PHISHING ATTACK BEFORE IT BEGINS

Before steps 1-5 above, a phisher must set up a domain to receive phishing data. Preemptive 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 emails authentication technologies become more widespread, email authentication could become a valuable preventive measure by preventing forged or misleading email return addresses.

## VI. 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, withdrawls, 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.

**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.

**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 unauthorised imagery in emails.

## VII. 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 authorised to send a message from a 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.

## VIII. DEFENCE FROM USERS POINT OF VIEW

**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.

**Verify the SSL Certificate**

Make sure to verify the SSL Certificate over the domain is there and do belong 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 icon.

**Inbuilt 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 use. For example, in case of Mozilla Firefox, Firefox 3 or later contains built-in phishing and Malware protection to help keep you safe online.

**Internet security Programs**

Many antivirus 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.

**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.

**Verifying the IP address of the host**

In case 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.

## IX. 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. 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 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.

## X. REFRENCES

[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, Willey Publishing, Inc. 2005
[5] http://www.justice.gov/opa/report_on_phishing.pdf