JRITM
JOURNAL OF RESEARCH AND INNOVATION IN TECHNOLOGY, COMMERCE AND MANAGEMENT

Journal of Research and Innovation in Technology, Commerce and Management
Vol. 3 Issue 4, April 2026, pp. 34001-34008
ISSN: 3049-3129(Online)

An Examination of Cybercrime in India

Prof.Uma Bharti
Assistant Professor, Parul Institute of Computer Application
Email: umas5381@gmail.com

Cite as: Prof.Uma Bharti. (2026). An Examination of Cybercrime in India. Journal of Research and Innovation in Technology, Commerce and Management, Vol. 3(Issue 4), 34001–34008. https://doi.org/10.5281/zenodo.19381910

DOI: https://doi.org/10.5281/zenodo.19381910

The term "cybercrime" describes crimes committed through the use of a communication channel or device, such as a watch, laptop, desktop computer, PDA, mobile phone, or car, either directly or indirectly. In the "Global Risks for 2012" research, cyberattacks are expected to be among the top five worldwide threats to the government and corporate sectors. Cybercrime is a kind of crime that gradually damages victims' life and is hard to detect and stop once it has occurred. Because online banking and shopping are becoming more and more popular and entail sensitive financial and personal data, we hear this phrase in the news a lot. In this paper, the various forms of cybercrime, their evolution, case studies, majors that focus on prevention, and the departments that fight them are briefly summarized.

1. Introduction

For law enforcement personnel, cybercrime is a relatively new threat. As more people own computers and are linked to the internet, there is a greater potential for cybercrime.The graphic below, which represents the most recent survey available for the year 2011, from "http://www.Internetworldstats.com," illustrates the global internet user population. Based on this data, we can deduce that Asia has the highest number of internet users worldwide. China is the nation most afflicted by internet fraud worldwide, according to the case study on this crime.

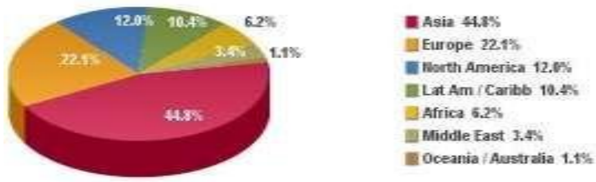


Figure 1: Global Internet users by region in 2011.

WORLD INTERNET USAGE AND POPULATION STATISTICS December 31, 2011						
World Regions	Population (2011 Est.)	Internet Users Dec. 31, 2000	Internet Users Latest Data	Penetration (% Population)	Growth 2000-2011	Users % of Table
Africa	1,037,524,058	4,514,400	139,875,242	13.5 %	2,988.4 %	6.2 %
Asia	3,879,740,877	114,304,000	1,016,799,076	26.2 %	789.6 %	44.8 %
Europe	816,426,346	105,096,093	500,723,686	61.3 %	376.4 %	22.1 %
Middle East	216,258,843	3,284,800	77,020,995	35.6 %	2,244.8 %	3.4 %
North America	347,394,870	108,096,800	273,067,546	78.6 %	152.6 %	12.0 %
Latin America / Carib.	597,283,165	18,068,919	235,819,740	39.5 %	1,205.1 %	10.4 %
Oceania / Australia	35,426,995	7,620,480	23,927,457	67.5 %	214.0 %	1.1 %
WORLD TOTAL	6,930,055,154	360,985,492	2,267,233,742	32.7 %	528.1 %	100.0 %

Figure 2:World internet users.

To have a better understanding of cybercrime, we have spoken about the terminology that are used in the field [2].

A. The Web

Millions of computers are connected by this worldwide network. Email, webpage access, chat, file transfers, and other uses are all done using it.

B. Internet Explorer

a program for using the World Wide Web server's information resources. Awebpage's address, or URL, is used to identify an information resource such as photos on a webpage.

C. Web proxy

Users can access the internet through an ISP (Internet Service Provider).

D. IP address

Every device linked to a computer network is given an IP (Internet Protocol) address, which acts as a unique machine identity. Take 172.17.64.150, for instance.

E. Spoofing IP addresses

It is sometimes referred to as IP address forging, in which an intrusive party obtains a compromised user's IP address to carry out their malicious activity. The hijacker targets the legitimate user, using the genuine's IP address to change the packet headers so the legitimate looks to be the original source [1].

F. Phasing emails

email address hacking. Email spoofing is the term used when a hacker utilizes a user's email address for malicious purposes [2].

G. Virus on computers

A computer application that is installed on a user's computer and that operates against the user's will and has the capacity to harm and duplicate files.

H. Worm on computers

These are the computer programs that propagate to other computers by self-replicating. Usually, because of the target computer's security flaws, it spreads across a network. It differs from a virus in that it doesn't require attachment to an already-running software, whereas viruses are limited to operating on the target machine.

I. Phishing

It's an attempt to pilfer private data. For instance, a user could get an email asking for their bank account information, PAN number, and the payment of 5000 INR in order to process their lottery winnings in the UK [3], [6].

J. Malware

It is malicious software that is unintentionally installed on a user's computer with the goal of gathering personal data about them.For instance, keyloggers2.

K. Worm on computers

These are the computer programs that spread to other computers by self- replicating.

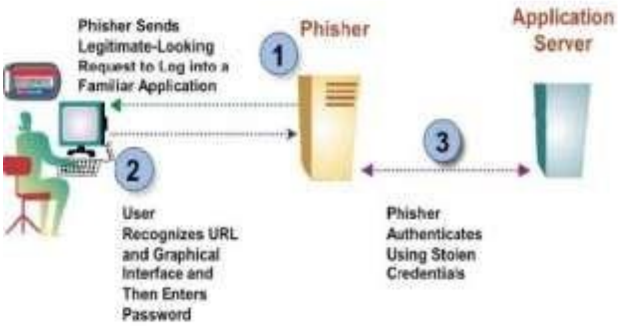
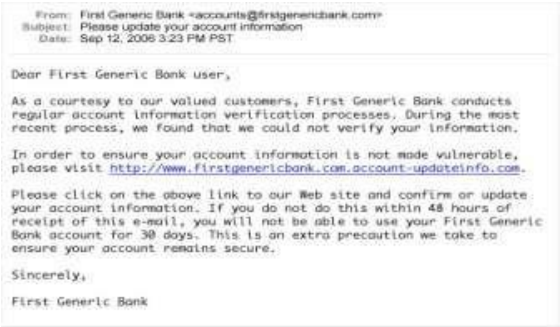


Figure 3: Block diagram of the Phising process

Journal of Research and Innovation in Technology, Commerce and Management
Vol. 3 Issue 4, April 2026, pp. 34001-34008
ISSN: 3049-3129(Online)



From: First Generic Bank <accounts@firstgenericbank.com>
Subject: Please update your account information
Date: Sep 12, 2006 3:23 PM PST

Dear First Generic Bank user,

As a courtesy to our valued customers, First Generic Bank conducts regular account information verification processes. During the most recent process, we found that we could not verify your information.

In order to ensure your account information is not made vulnerable, please visit http://www.firstgenericbank.com.account-updateinfo.com.

Please click on the above link to our Web site and confirm or update your account information. If you do not do this within 48 hours of receipt of this e-mail, you will not be able to use your First Generic Bank account for 30 days. This is an extra precaution we take to ensure your account remains secure.

Sincerely,

First Generic Bank

Figure 4: An example of Phising

A Phishing example Usually, because of the target computer's security flaws, it spreads across a network. It differs from a virus in that it doesn't require attachment to an already-running software, whereas viruses are limited to operating on the target computer.

L. Adware

A malicious software that is unintentionally installed on a user's computer with the goal of gathering personal data about them. For instance, Keyloggers2.

II. The Development of Cybercrime.

The employees' traditional employment and means of survival were threatened by the advent of "Loom," a device invented in 1820 by textile manufacturer "Joseph- Marie Jacquard" that permitted the recycling of steps for weaving fabrics. The first cybercrime to be reported was this one. They thus launched a counterattack to discourage people from using the technology any more. Cybercrime includes more recent kinds of computer abuse such online defacement, hacking, web jacking, and cyberstalking in addition to more traditional criminal behaviors like theft, fraud, forgery, mischief, and defamation. The Asian School of Cyber Law's R Nagpal defines cybercrime as "unlawful acts wherein the computer is either a tool or a target or both." This definition covers a wide range of devices, including sophisticated watches, mobile phones, PDAs, and other gadgets. Without the aid of computers, the majority of modern crimes—such as the well-known attack on the "World Trade Center" in the United States, serial bombings, the "Taj" hotel in India, and online site hacking—would not be conceivable. Unfortunately, it is impossible to determine the precise impact of cybercrime on society and finance because the majority of cases go unreported. Intelligence agencies are working hard to prepare for cyberattacks because they may have terrible consequences, affecting financial markets, banking systems, and rail and air traffic controllers [7].

III. Cybercrime Types

A. Financial crimes
B. cyber pornography
C. the sale of illegal goods
D. Internet-Based Betting
E. Theft of Intellectual Property
F. Forgery
G. Email Spoofing
H. Cyber Defamation
I. Tracking via Cyberspace
J. Vandalism on the Internet
K. Bombing emails
L. Data fiddling
M. Attacks with Salami
N. Attacks that Cause Service Outages
O. Malware/Virus Assaults
P. Keyloggers & Trojan Horses

IV. Indian Cybercrime Cases

In the United States, incident reporting remains low.

During the first three years (1995–1997) of the CSI-FBI survey, just 17% of respondents reported incidences of cybercrime, according to an article by Rosemary Clandos. Although reporting has almost increased in previous years, it has 30%. According to a recent SS Gole newspaper story, Pune is currently ranked third among the cities afflicted by cybercrimes based on incidents reported in 2011. According to National Crime Records Bureau data, Vishakhapatnam registered 107 offenses, and Bangalore recorded 117 instances, making Bangalore the city most affected. The Indian Penal Code (IPC) and the Information Technology Act, 2000 are the two laws in India that allow for the booking of criminals. The IT Act of 2000 contains documents pertaining to hacking, unauthorized access, plagiarism, and other related topics, whereas the IPC contains classic crimes like mischief, defamation, theft, fraud, and forgery, among others.

SL. NO.	Crime Heads	Cases Registered				% Variation in 2010 over 2009	Persons Arrested				% Variation in 2010 over 2009
		2007	2008	2009	2010		2007	2008	2009	2010	
1	Tampering computer source documents	11	26	21	64	204.7	2	26	6	79	1216 7
2	Hacking with Computer System										
	i) Loss/damage to computer resource/utility	30	56	115	346	200.8	25	41	63	233	269.8
	ii)Hacking	46	82	118	164	38.9	23	15	44	61	38.6
3	Obscene publication/transmission in electronic form	99	105	139	328	135.9	86	90	141	361	156.0
4	Failure										
	i) Of compliance/orders of Certifying Authority	2	1	3	2	-33.0	1	2	6	5	-16.6
	ii) To assist in decrypting the information intercepted by Govt. Agency	2	0	0	0	@	0	0	0	0	@
5	Un-authorised access/attempt to access to protected computer system	4	3	7	3	57.1	0	1	16	6	-62.5
6	Obtaining licence or Digital Signature Certificate by misrepresentation/suppression of fact	11	0	1	9	800.0	11	0	1	4	300
7	Publishing false Digital Signature Certificate	0	0	1	2	100.0	0	0	0	2	@
8	Fraud Digital Signature Certificate	3	3	4	3	-25	3	0	6	4	33.3
9	Breach of confidentiality/privacy	9	8	10	15	50.0	3	3	5	27	440.0
10	Other	0	4	1	30	2900	0	0	0	17	@
	Total	217	288	420	966	128.4	154	178	288	799	177.4

Figure 5: Cyber Crimes/Cases Registered and Persons Arrested under IT Act during 2007 - 2010

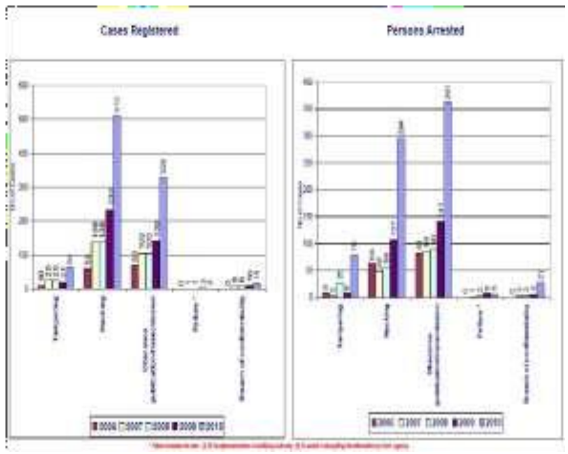
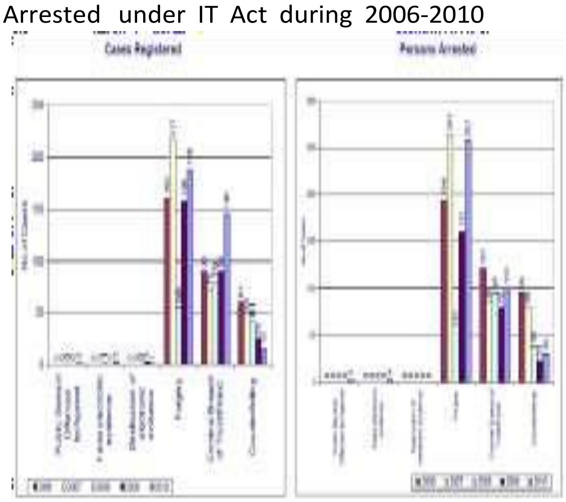


Figure 6: Cyber Crimes / Cases Registered and Persons Arrested under IT Act during 2006-2010



V. Analysis of Cases To apply and elucidate the phishing process[5].

A. Phishing study of websites An identical clone of the HSBC bank website was designed to comprehend phishing and its methods. The website's main goal was to employ phishing emails to trick people into submitting their credentials (user name and password). The sample of the employees of HSBC Bank were taken after gaining the required permissions from

Journal of Research and Innovation in Technology, Commerce and Management
Vol. 3 Issue 4, April 2026, pp. 34001-34008
ISSN: 3049-3129(Online)

management. A phony link that was inserted in the email body and linked to the targeted 120 employees' original Cust ID and password, enabling them to check their account, alerted them to the risk associated with their account.

Answer to phishing mail	Exact target number of employees
Positive interaction (Income Tax Department)	8
Positive interaction (Other Departments)	44
Negative interaction (With incorrect info)	28
Negative interaction (With no response)	40
Sub Total	120

Table1: Website phishing analysis

1.1 Phishing Email Deception The bank's cyber division has recently reviewed your accounts and found evidence that an outside entity is attempting to gain access. Our top priority is keeping our network safe. The services connected to your account that were at risk of being compromised have been terminated in order to preserve integrity. In order to verify your identity and get the account reactivated, we kindly ask that you check in using the previous set of credentials. Following login, the following notice will show up on the screen:

"This is to notify you that the information you submitted has been successfully updated in the bank's central database."

•To begin, kindly adhere to the guidelines provided here:

If there has been any inconvenience, please click https://www.hsbcindia.com. We value your time and thank you for your rapid attention in helping us to protect the integrity of the financial system.

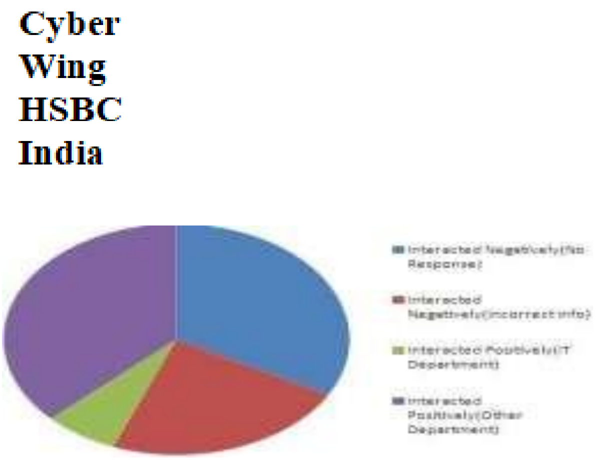


Figure 8: Deceiving Phishing Email

Out of 120 respondents, 44% answered positively and logged in using their login credentials (customer ID and password). Remarkably, 8 out of 120 victims, or 7%, were income tax department workers and auditors. These results were unexpected since we had assumed that they would be more knowledgeable about cybercrime preventive techniques. While working through other departments, we were able to capture 37% of those who immediately supplied the account's credentials. When we finally divided 56% (68 out of 120), the outcomes were as follows: Since the information provided by them was determined to be inaccurate, it was discovered that 23% (28 employees) had received training at the highest level for security majors; 33% (40 employees) did not answer at all to the

Journal of Research and Innovation in Technology, Commerce and Management
Vol. 3 Issue 4, April 2026, pp. 34001-34008
ISSN: 3049-3129(Online)

information they were given. Nearly half of the employees who replied were victims of phishing, which is a clear sign that the phenomenon is dangerous (figure 2),
especially for trained professionals like those in the IT department and IT auditors. Raising everyone's knowledge of this risk factor who uses e-banking is strongly advised; this applies to both clients and staff.

B, Analysis of phone phishing Female coworkers lured all fifty of the target employees with the intention of obtaining user credentials for their individual bank accounts. The outcome much beyond our expectations; many of them were brought down by this ruse. They disclosed their credentials after a positive conversation for fictitious reasons, such as verifying their access and privileges, ensuring account security and privacy, and addressing integrity and connection problems, among other things. After contacting us three or four times in an attempt to make our request appear genuine, 32% of the employees—16 out of 50—were tricked into giving away their login information for their online banking account. We were surprised by this high percentage because the target members came from the banking industry, which is supposed to be far more risk averse when it comes to e-banking services. The remaining 52% (26 employees) declined to disclose the credentials since they were prepared with the precautionary majors against cybercrime, while 16% (8 employees) disclosed their user name and were excused from sharing passwords.

Phone Phishing Experiment Response	**Exact Number Of Employees**
Sharing full credentials	16
Sharing only user name	8
Refused for any information	26
Sub Total	50

Table1: Phone phishing analysis

Figure 1 results provide a clear image of the security factor related to social engineering, which is made up of direct risks to the e-banking web service since it allows for the direct hacking of an e- bank customer's account.

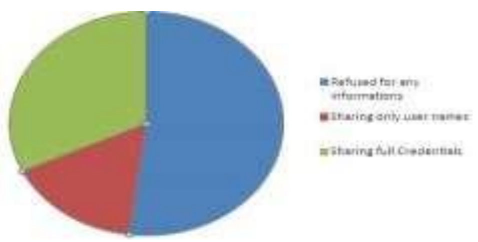


Figure 9: Phone Phishing Analysis

B. Analyzing the experiments responses

We recognized that every employee who had been caught in the phishing practice had not responded, having never realized it was a phishing attack; the employees who had not been caught had either never seen the email—since most email servers consider these to be spam—or had recognized the phishing attack and had not responded. A greater number of users believed the study had no value and felt violated because they had not been asked permission before the experiment was conducted, even though some subjects recognized the educational value of the experience and valued the insights they had gained as a result of participating in the study. It's interesting to note that not a single employee acknowledged falling for the phishing scheme or spoof email. Instead, those who expressed anger did so either on behalf of a friend who was duped or in more general terms. This implies that being a victim carries a distinct stigma, regardless of whether actual harm was caused, which tells us to be wary of the findings of phishing surveys (Peter Finn and Markus Jakobsson, 2006). Some employees referred to the experiment as fraudulent, illegal, inappropriate, and unethical, demonstrating that phising is linked to significant psychological costs for the victims. They were accusing phishers of violating people's privacy even though personal data was not kept. Many workers claimed they could never fall victim to such attacks, indicating that we are not yet ready to acknowledge our own vulnerability. Consequently, the majority of the effects go unreported. These responses demonstrate that some users are unaware of the possible consequences of the information they voluntarily divulge online.

They find it unclear that anyone can easily obtain their personal information (without violating any ethical standards) and that, for the most part, there are no repercussions for those who violate them. We came to the conclusion that phishers are well aware of the fact that most users are ignorant of security procedures and, as a result,

they believe websites requesting personal information to be authentic. It can be challenging for users to distinguish between a real and fake security major if they are unaware of their level of security and assume that they are.

The results demonstrate the ineffectiveness of certain visual deception attacks on a large user base and recommend the adoption of alternative strategies. Some of these attacks can even fool the most knowledgeable users. A considerable number of participants failed to recognize the reliability of the indicators that were intended. Some people only used the contents of the website to verify authenticity, rather than using the entire browser. Regarding padlock, some participants felt that it would work better if it was shown within the page when the browser presented it. When compared to SSL indicators, some users were more convinced by animated graphics, design elements like favicons and URL bar icons, and images. If phishers are aware of these details, they can manipulate a fully functional and loaded website by adding images of security indicators, logos, and links. This will make a significant portion of the spoof website appear authentic.

Similar to this, respectable companies who adhere to security standards, such as permitting users to access their accounts only through SSL-protected websites, are penalized and seen less reliable. Campaigns to raise awareness and educate the public about the various tactics used by cybercriminals

are desperately needed. The only way to lessen the risk of personal information being misused is to raise awareness.

VI. Concluding Remarks

We have discussed several facets of cybercrime in this essay and included case studies to back up our arguments. We might conclude that, when compared to traditional crimes, cybercrime is far more horrible and destructive. Given the current growth scenario, which is entirely reliant on computers, every country and its citizens will need to be knowledgeable about cybercrime, criminal psychology, and the laws that govern it. "You should hack yourself in order to protect yourself from hackers."

VII. Recognition

We express our gratitude to the cyber lawyers, cyber police, bankers, and scientists who have contributed to the fight against terrorism, raising awareness of cybercrime, and sharing important information through print and electronic media, all of which have greatly aided our research.