Cyber Security for Individuals in India

Krishna Kumar[1] Rachna Shah[2] Dr. A. C. Joshi[3]
[1]Assistant Engineer (R&D) [2]Scientist-B [3]Director (HR)
[1]UJVN Ltd., Ganga Bhawan, Dehradun, Uttarakhand, India [2]NIC State Unit, Dehradun, Uttarakhand, India
[3]UJVN Ltd., Ujjawal, Maharani Bagh GMS Road, Dehradun, Uttarakhand, India

Abstract— As per Indian Computer Emergency Response team (CERT-IN), one cybercrime was reported every 10 minutes in India during 2017-18, this statistic is quite alarming and therefore, merits a focused and collective attention of security enforcement agencies [1]. This paper explores the nature of groups engaged in cybercrime. It briefly outlines some of the frequent cybercrime activities used by frauds. The paper is based on the real case studies. It is apparent that a wide variety of organizational structures are involved in cybercrime.

Keywords: CIBIL, Cyber Crime, Forgery, PAN Card

I. INTRODUCTION

Cyber Crime is not defined in I.T. Act 2000 neither in the I.T. Amendment Act 2008 and nor in any other legislation in India. To define cybercrime, we can say, it is just a combination of crime and computer. To put it in simple terms ‘any offense or crime in which a computer is used is a cybercrime’. Interestingly, even a petty offense like stealing or pickpocket can be brought within the broad purview of cybercrime if the basic data or aid to such an offense is a computer or any information stored in a computer used (or misused) by the fraudster.

II. PRESENT SCENARIO ON CYBER SECURITY

S.No.	Cyber Crime	2017	2016
1	Online Banking	2,095	1,343
2	Facebook Related	316	151
3	Email hacking	121	97
4	Sexual harassment	81	51
5	Lottery Fraud	42	15
6	Data theft	47	43
7	Job Fraud	49	40
8	Twitter Related	12	04
	Total Cases	3,474	2,402

Table 1: Rise in Cybercrime [1]

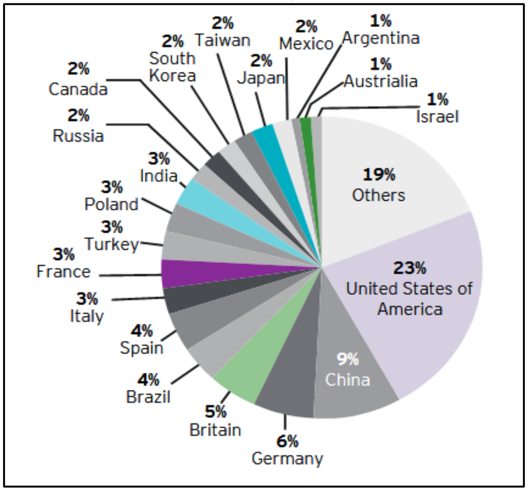

Fig. 1: Top 20 Countries Impacted by Cybercrime [1]

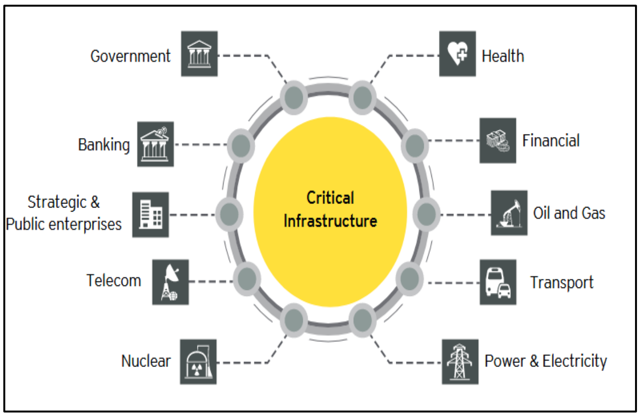

Fig. 2: Critical Infrastructure targeted in Cyber crime

Account hacking program	US $12.99
Hacked Instagram accounts in bulk	1000-10,000 accounts US $15- US $60
Botnet:Blow-bot banking botnet	Monthly Basis Rental US$750 Monthly Full Rental US$1200 Monthly Support US$150
Disdain exploit kit	Day US$80, week US$500, Month US$1400
Stegano exploit kit, Chrome, Firefox, Internet Explorer, Opera, Edge	Unlimited traffic, day US$2,000 Unlimited traffic, month US$15,000
Microsoft office exploit builder	Lite exploit builder US$650 Full version US$1,000
WorldPress exploit	US$100
Password stealer	US$50
Android malware loader	US$1,500
DDOS attacks	Week long attack US$500-US$1,200

Table 2: Rates of cybercrime as-a-service [1]

III. INDIAN INFORMATION TECHNOLOGY ACT

The Information Technology Act -2000 and the I.T. Amendment Act 2008 in general and with particular reference to banking and financial sector related transactions. In India cybercrime cases are registered under three broad categories they are Information technology act, Indian penal code, and other State Level Legislations (SLL). The following are the cases registered under IT Act.

- Tampering of electronic documents – sec. 65 of IT Act
- Loss or damage to computer utility or resource – sec 66(1)
- Hacking – sec. 66(2)
- Electronic obscenity – sec. 67
- Failures of order of certifying authority – sec. 685
- Unauthorized access to computer system – sec. 70

- Misrepresentation – sec. 71
- Fake digital signature publishing – sec. 73
- Fake digital signature – sec. 74
- Privacy/confidentiality breach – sec. 72

A. Case Studies:

1) Case-I:

A group of people was involved in a forgery case, they found details such as PAN card number, name and father's name, and by using these details they took 05 consumer loans, one credit card, and one car loan from four different banks. The person was unaware of the loans, but came to know about it when he went to the bank for KYC updation to start SIP. After knowing about the forgery he visited Police station cybercrime branch and made a written complaint. After the investigation, they found that PAN card and voter ID card were used for taking loans, fraudies edited his details on any other PAN card and voter ID. Signature and photograph on the PAN card were not his and after investigation an FIR was filed.

A written complaint to all the banks was made by him through email with a copy of FIR. Banks investigated the details from their end and accepted that loans were not taken by him and removed all the loans from his CIBIL profile.

To avoid this type of cybercrime, always check your CIBIL profile only on www.cibil.com website, after providing some basic details for registration, you can check your CIBIL report/profile free once in every year for one month and more than once on paid basis. CIBIL profile shows all the details like your home address, your office address, details of loans, payment status of loans, details of banks visited your profile for inquiry of loans.

After checking the CIBIL profile if you are satisfied with your CIBIL details, then you are the happiest person and if you find that any loan which was not taken by you is being reflected in your CIBIL profile then the same should be reported through your CIBIL profile. If CIBIL responded that the reported loans do not belonging to you and suppressed from your CIBIL profile, then, it's ok.

But if reply from CIBIL after cross verification from the bank is negative and they inform that, the loan belongs to you, means you are in trouble and someone has used PAN card details to take the fake loan. In this case firstly file an FIR in your nearest police station and after getting a copy of FIR write a complaint to the bank through email with attached copy of the FIR. If the bank is a PSU bank then you can also make an online complaint to the central vigilance committee (CVC). If your matter is resolved by the bank then its ok, but if the bank does not take any action or you are not satisfied with their reply, then you can make written complaint to your nearest banking ombudsman (RBI).

2) Case-II:

Most of the people use Gmail during first time registration in mobile phone for saving data and contact numbers. I did the same and one day I lost my mobile phone. To avoid any misuse of my crucial and important data, I used the features which are already available in Gmail.

To check the available facilities of Gmail follow the following steps:

1) Open your Gmail account which syncs with your mobile phone.
2) Then, click on account.
3) Then, click on security.
4) Click on "Find a lost or stolen phone":

The following options are available for your mobile phone.

a) Ring your phone.
b) Locate your phone.
c) Lock your phone.
d) Sign out on your phone.
e) Reach out to your carrier.
f) Consider erasing your device.

IV. CONCLUSION

Nowadays information technology is playing a major role in our day to day life, without IT we are not going to do any work. The increase use of technology will also lead to increase in cybercrime rate. The cybercrime cases has to be handled very carefully in order to cull out the truth. Providing awareness to people and training to the police and judicial officers is very important. To study forensic and cyber related issues, Gujarat Forensic Sciences University has been started by Govt. of Gujarat which is the world's first and only University dedicated to Forensic and allied Sciences.

REFERENCES

[1] Report on "confronting the new-age cyber-criminal" by FICCI, Federation House, Tansen Marg, New Delhi.

[2] M. Elavarasi and N. M. Elango, "Analysis of Cybercrime Investigation Mechanism in India", Indian Journal of Science and Technology, Vol 10(40), DOI: 10.17485/ijst/2017/v10i40/119416, October 2017.

[3] Roderic Broadhurst, Peter Grabosky, Mamoun Alazab & Steve Chon, "Organizations and Cybercrime: An analysis of the Nature of Groups engaged in Cybercrime", International Journal of Cyber Criminology, Vol 8 Issue 1 January - June 2014.