



Export Promotion Council for Handicrafts

EPCH HOUSE, POCKET 6 & 7, SECTOR 'C', LOCAL SHOPPING CENTRE, VASANT KUNJ, NEW DELHI-110070

Tel: 91-11-26135256

Fax: 91-11-26135518,26135519

Email : focusregion@epch.com

web : www.epch.in

REPORT ON AWARENESS SEMINAR ON “HOW TO SAFEGUARD YOUR BUSINESS FROM CYBER CRIME DURING ONLINE TRANSACTION” ON 1st AUGUST, 2015”, AT THE CONFERENCE HALL, 3RD FLOOR, RAJIV GANDHI HANDICRAFT BHAVAN, BABA KHARAK SINGH MARG, CONNAUGHT PLACE, NEW DELHI

The Export Promotion Council for Handicrafts regularly conducts seminars for its member exporters to educate them on new and emerging issues related to exports. On 1st August, the Council organised a seminar on a very important issue: **How to Safeguard Your Business from Cyber Crime during Online Transaction**” at the Rajiv Gandhi Handicrafts Bhavan, Baba Kharak Singh Marg, Connaught Place, New Delhi.



Mr. Mohit Kumar interacting with participants



The seminar was attended by more than 35 delegates from different export houses. The seminar was presided over Mr. Rajesh Rawat (Deputy Director, EPCH) and the guest speaker for the event was Mr. Mohit Kumar from KPMG, Gurgaon.

Mr. Mohit, discussed about the importance of using safe online transaction. Mr. Mohit said that Computer crime, or cybercrime, is any crime that involves a computer and a network of computers. The computer may have been used in the commission of a crime, or it may be the target. Netcrime is criminal exploitation of the Internet, inherently a cybercrime.

Issues surrounding these types of crimes have become high-profile, particularly those surrounding hacking, copyright infringement, banking fraud etc. There are also problems of privacy when confidential information is intercepted or disclosed, lawfully or otherwise.

Computer fraud is any dishonest misrepresentation of fact intended to let another to do or refrain from doing something which causes loss. In this context, the fraud will result in obtaining a benefit by altering, destroying, suppressing, or stealing output, usually to conceal unauthorized transactions. A variety of internet scams, many based on phishing and social engineering, target consumers and businesses also.

Questions put up by the audience –

Q.What is Cybercrime?

Ans: Cybercrime refers to all the activities done with criminal intent in cyberspace. These could be either the criminal activities in the conventional sense or could be activities, newly evolved with the growth of the new medium. Because of the anonymous nature of the Internet, it is possible to engage into a variety of criminal activities with impunity and people with intelligence, have been grossly misusing this aspect of the

Internet to perpetuate criminal activities in cyberspace. The field of Cybercrime is just emerging and new forms of criminal activities in cyberspace are coming to the forefront with the passing of each new day.

Q. Is hacking a Cybercrime?

Ans: Hacking and cracking are amongst the gravest Cybercrimes known till date. It is a dreadful feeling to know that a stranger has broken into your computer systems without your knowledge and consent and has tampered with precious confidential data and information. Coupled with this, the actuality is that no computer system in the world is hacking proof. It is unanimously agreed that any and every system in the world can be hacked. Using one's own programming abilities as also various programmes with malicious intent to gain unauthorized access to a computer or network are very serious crimes. Similarly, the creation and dissemination of harmful computer programs which do irreparable damage to computer systems is another kind of Cybercrime. Software piracy is also another distinct kind of Cybercrime which is perpetuated by many people online who distribute illegal and unauthorised pirated copies of software.

Q. Is there any comprehensive law on Cybercrime today?

Ans: Since Cybercrime is a newly specialised field, a lot of developments have to take place in terms of putting into place the relevant legal mechanism for controlling and preventing Cybercrime. As of now, there is absolutely no comprehensive law on Cybercrime anywhere in the world. This is reason that the investigating agencies like CBI are finding the Cyberspace to be an extremely difficult terrain. These various Cybercrimes fall into that grey area of Internet laws which is neither fully nor partially covered by the existing laws and that too in some countries.

Q. Why do we need to fight Cybercrime?

Ans We all must remember that Cyberspace is a common heritage of ours which we have inherited in our life times from the benefits of ever growing technologies. This Cyberspace is the lifeline of the entire universe and given its irreversible position today, it is the duty of every netizen to contribute toward making the said cyberspace free of any trouble or cybercrime.

We welcome suggestions and feedback to make this initiative more productive. Do write to us at: focusregion@epch.com.

Cyber Security

Mohit Kumar

#root@localhost: whoami

Mohit Kumar is a passionate Information Security consultant with more than 5 years of experience. He is a Bachelor of technology, Certified Ethical Hacker (CE|H), Certified Hacking Forensic Investigator (C|HFI) and CISCO Certified Network Associate. Mohit started his career as a freelance cyber security and forensic expert for countries prestigious law enforcement and regulatory authorities like Income Tax Department, Directorate of Revenue Intelligence, Delhi Police etc. He is now a part of Big-4 consultancy Firm and works as a Cyber Forensic Investigator dealing in corporate frauds pertaining to multi-national and listed companies. At the age of 21, he found a major vulnerability in Facebook which was also published in Times of India and was shared across social media. He has Trained 200+ Indian Revenue Services officers in a workshop hosted at National Academy of Custom Excise and Narcotics, Faridabad about cyber forensics & cyber security. He has also trained 100+ officers of IT cadre of Delhi E-Governance Society of Delhi Government in Cyber Security. He has been interviewed by India Today group channels on the subject of Cyber Security & Cyber Forensics on several occasion.

Cyber Crime

Cyber Crime(Def) : Dr. Debarati Halder and Dr. K. Jaishankar (2011) define Cybercrimes as: "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS)". Such crimes may threaten a nation's security and financial health.

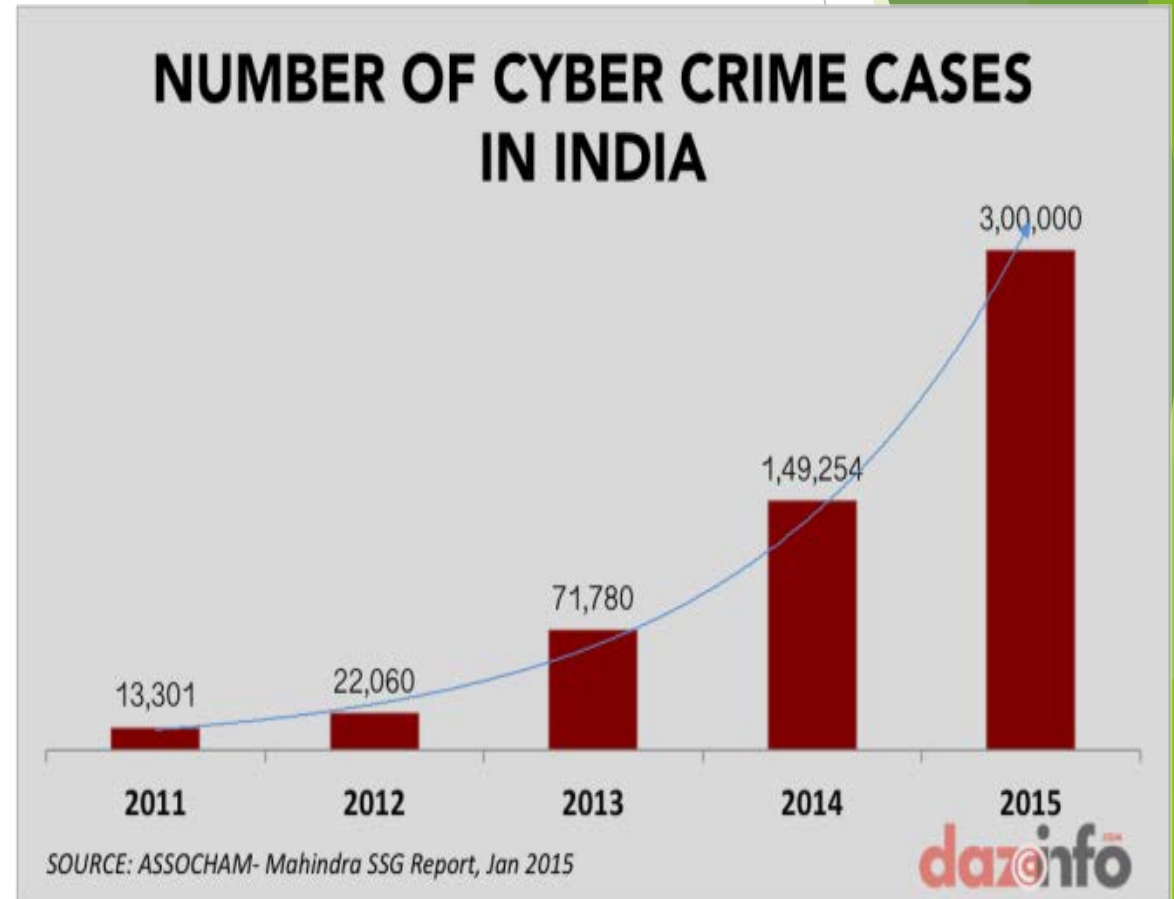
(Source: Wikipedia)

Why cybercrimes are committed ?

- ▶ Thrill.
- ▶ No physical contact is required.
- ▶ Financial gain.
- ▶ Confidential and privileged Information.
- ▶ Spreading virus to large number of computers.
- ▶ Lack of security of digital devices.
- ▶ IP Theft.

Cyber Crime scenario in India

Assocham-MahindraSSG study suggests that Cyber Crime is increasing at an alarming rate. According to the report, the number of Cyber Crimes in India may touch a humongous figure of 3,00,000 in 2015 while it was 1,49,254 in 2014.



Network Interface Card

- Allows a network capable device access to a computer network such as the internet.
- The MAC address identifies the vendor and the serial number of the NIC which is unique to the card. Also referred as Ethernet.



Network Hub

- A network hub or repeater hub is a device for connecting many twisted pair or fiber optic Ethernet devices together.
- When a packet arrives at one port, it is copied to all the ports of the hub for transmission



Network Switch

- A switch is a device that performs switching.
- It forwards and filters datagrams (chunk of data communication) between ports based on the Mac-Addresses in the packets.



Router

- Forward data packets between networks using headers and forwarding tables to determine the best path to forward the packets.
- Generally accessible on the gateway I.P
e.g: if IP is 192.168.1.5 then type 192.168.1.1 in the browser.



Classification of I.P Address

Dynamic IP addresses are those that change when you switch OFF and switch ON your router. IP address keeps changing every time you switch on your computer. Dynamic I.P were introduced because the ISP's pool of I.P is getting exhausted. As soon as you switch off your computer/router your I.P address is allotted to some other user that logs in freshly.

Static I.P addresses are those that never change even if you restart your computer/router. These are fixed for a computer. Webservers/email servers have a static I.P address.

Domain Name Server

- Associates various information with domain names. Resolve hostnames to I.P addresses.
- It serves as the "phone book" for the Internet by translating human-readable computer hostnames.
- If DNS would have not been present then for you google.com would have been 74.125.236.34 and facebook would have been 173.252.110.27.
- People who want to be more secure & faster internet can use Google's DNS servers:
Primary DNS : 8.8.8.8
Secondary DNS: 8.8.4.4

Modes of Attack

Phishing

Spear
Phishing

Email
Spoofing

SMShing

Social Media
Chat

OS
Vulnerability

Wifi Attacks

Network
Attacks

Stolen
Device

Cookie
Grabbing

Similar
domain
registration

Malicious
intention of
employee

Prevention is Better than Cure

On Screen
keyboard

Different
Passwords

Software Updates

Antivirus

Antispyware

Boot Level
antivirus scan

Avoid usage of
public WiFi

Use of VPN

Firewall

Endpoint Security

Restricted access
to websites

One Time
Passwords

IT Audits

Use SSL

Inform Bank and
clients of no
change in account
no/address.

QUESTIONS?

A Gentleman never asks...
A woman never says...

Thank You..

Reach out to me at:

Email: mohitakumar@icloud.com

Mobile: +919873140114