INFORMATION TECHNOLOGY ACT 2008 AT THE VERGE OF PROTECTING E-COMMERCE FROM CYBER CRIMES

AKHIL BHUSNUR, AKHILA WALI

Abstract: Crime is as old as the society. The form of crime is changing with the advancement in technology. Crime and its perpetrators are now using computer and gadgets as a tool to commit criminal activities. Crime is an offence which is committed by an individual or a group of individuals which is punishable by the law. Most trending crime is CYBER CRIME. Cyber crime is a crime wherein a computer is being used to commit a crime. These are the offences which are committed by an individual or a group or individuals with the means of computer with malafide intentions, and cause physical or mental harms or loss to the victim directly or indirectly. Cyber Theft, Cyber Stalking, Identity Theft, and the, most important of all Hacking, are some of the different types of Cyber Crimes in the recent years. Hacking among all types of cyber crime it is the most dangerous and serious threat to the internet and e-commerce. Hacking refers to breaking into the computer and steal valuable data from the system without any permission. Persons involved in Hacking are known as Hackers. In the recent years, incidents of hacking are increasing day by day. Hacking is governed by Information technology Act 2008 in India, and the said Act also prescribes different punishments for various cyber crimes. The present article gives an insight into the world of Hacking and the legal protection from Hacking.

Introduction: The word "CRIME" has a general meaning as a 'legal wrong that can be followed by criminal proceedings which may result into punishment' whereas CYBER CRIME may be 'unlawful acts wherein the computer is either a tool or target or both'.

Cyber crime is an offence which is committed by an individual or a group of individuals with the means of computer with malafide intentions, and cause harm to the victim and hence is a punishable offence. Cyber Theft, Cyber stalking, Identity Theft and the most important of all is "HACKING", hacking has become a serious threat to the society. Even though laws and precautionary measures are always taken to keep information safe in the computers but still there are several cases in this present situation wherein highly confidential information is hacked and misused.

Hacking, What Is It?: Hacking refers to breaking into the computer with malafide intentions in order to intrude into the confidential information. It is amongst the gravest cyber crimes till date.

Hackers, Who Are These?: A person who hacks computers is called Hackers. But the word Hacker was actually used for a person who was highly knowledgeable in computer and technology. But off late due to media hype the word Hacker is used for as a negative word and is prevailing in the same fashion till date.

Types Of Hackers: There are three types of hackers and they are White hat hacker, Grey hat hacker and Black hat hacker.

White hat hacker also known as ethical hackers or a computer security expert. Who specializes in penetration testing and in other testing methodologies to ensure the safety and security of an organizations information system. When a white hat hacker discovers some vulnerability, they will exploit it only with permission and not divulge its existence until it has been fixed.

Grey hat hacker, they are computer hacker or computer security expert who may sometimes violate laws or typical ethical standards, but doesn't have the malicious intention. When a grey hat hacker discovers some vulnerability they will neither illegally exploit it, nor tell others how to do so.

Black hat hacker, they are the persons who violates computers security for little reason beyond maliciousness or for personal gain. When a black hat hacker discovers some vulnerability, they will illegally exploit it and or tell others how to do so.

How Did It Begin?: In 1820, Joseph Marie Jacquard, a textile manufacturer in France, produced the loom. This device allowed the repetition of a series of steps in the weaving of special fabrics. This resulted in a fear amongst Jacquard's employees that their traditional employment and livelihood were being threatened. They committed acts of sabotage to discourage Jacquard from further use of the new technology. This is the first recorded cyber crime.

The world 1st computer specific law was enacted in the year 1970, by the German State of Hessen in the form of Data Protection Act 1970, with the advancement of cyber technology.

In R. v. Gold prestel systems, it provided subscribes free e-mail facilities and access to its database.

Worm Attack: The Robert Tappan Morris well Known as First Hacker, Son of former National Security Agency Scientist Robert Morris, was the first person to be prosecuted under the 'Computer and Fraud Act, 1986'.

26 January, 2016 – The County of San Diego has confirmed that the classified records of all the employees were accidently sent to Wells Fargo as opposed to only those that are set up for Health Savings Accounts with the latter. The County and Wells Fargo are working together to delete unwanted records. A three year-long credit monitoring has been offered to the affected people. The breach is being deemed as an accidental error due to incorrect program code for data transfer by Hewlett- Packard Enterprise Services.

Against Hacking In The 21st Century: The first ever law made against hacking was in the year 1980 in USA. The Computer Fraud and Abuse Act (CFAA) were enacted by congress in 1986 as an amendment to existing computer fraud law, which had been included in the Comprehensive Crime Control Act of 1984.

And in India we got the first ever cyber crime law in 2000 that is Information and technology Act 2000 which does not include the hacking offence directly. However the amended form of this above act includes hacking that is Information and Technology act 2008 (ITA A 2008)

The US Congress passed the Cyber security Act of 2015, and President Barrack Obama signed the measure into law on December 18, 2015. The Act of 2015 aims to defend against cyber attacks by creating a framework for the voluntary sharing of cyber threat information between private entities and the federal government, as well as within agencies of the federal government. And all the other countries have their own laws against hacking like for example Australia has Australian cyber crime act 2001, and so on.

Some of the organizations have up in order to help the victims of hacker, for example there is Information Systems Audit and Control Association (ISACA) in USA, National Consumer Disputes Redressal Commission (NCDRC) in India. Cyber security Nexus (CSX) program, ISACA is committed to providing security professionals with the knowledge, guidance and tools they need to help and be effective at their job. We closely monitor legislation affecting cyber security, and are poised to keep you up-to-date on significant developments via news on this web page. It's just one of the ways we're working to be your premier resource for all things cyber security.

NCDRC will be setting up research centers across the country in collaboration with various colleges and universities, with the following primary objectives: To encourage students who would like to take up a career in cyber security. To provide students with hands on environment, so they can practice what they learn.

Indian Computer Emergency Response Team (CERT-In) and Centre for Development of Advanced Computing (CDAC) are involved in providing basic and advanced training to Law Enforcement Agencies, Forensic labs and judiciary on the procedures and methodology of collecting, analyzing and presenting digital evidence.

Even then, the numbers of hacking cases are exists and are increasing day by day! In the 21st century, the more the technology is increasing so is the crime, even after having laws. Hacking, the highly confidential files of the government or army or navy or air force or maybe even a company is a serious threat to the nation itself because the later consequences are unimaginable. This may lead to cyber terrorism and what not. And for a matter of fact such cases are increasing considerably.

With the out spread of terror all around it is not affordable to provide an easy platform for intruding into the Confidential files. The amount money lost is also huge.

The above graphs clearly indicate that the though there have been laws against cyber crime and hacking especially there has no decline in the crimes but has be increasing day by day or must say minute by minute. May be because of the vague laws and less punishment the hacker's strength to increase hacking is increasing day by day.

Cyber Crime Against Children – A new threat to the society, which speaks about the cyber crime happening against children especially girls. Here Hacking is being defined in a bit different manner, that how a girl's computer can be hacked and later how her personal information like pictures and documents can be misused, which further leads to heinous offences.

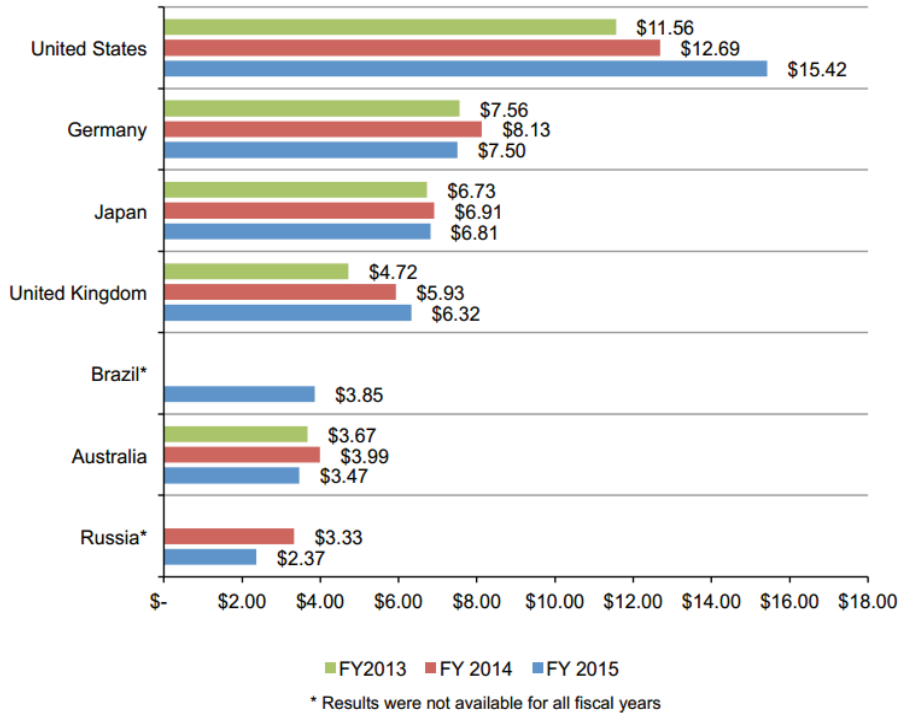
"Cybercrime cases in India increased by 69% in 2014", said Ravi Shankar Prasad in 2014. Cybercrime cases in India rose 69 per cent in 2014 year-on-year with 9,622 cases registered under the IT Act.

"Cyber crime has become a big threat for the country", said Rajnath Singh in Inaugurating an information security conference — 'Ground Zero Summit-2015'.

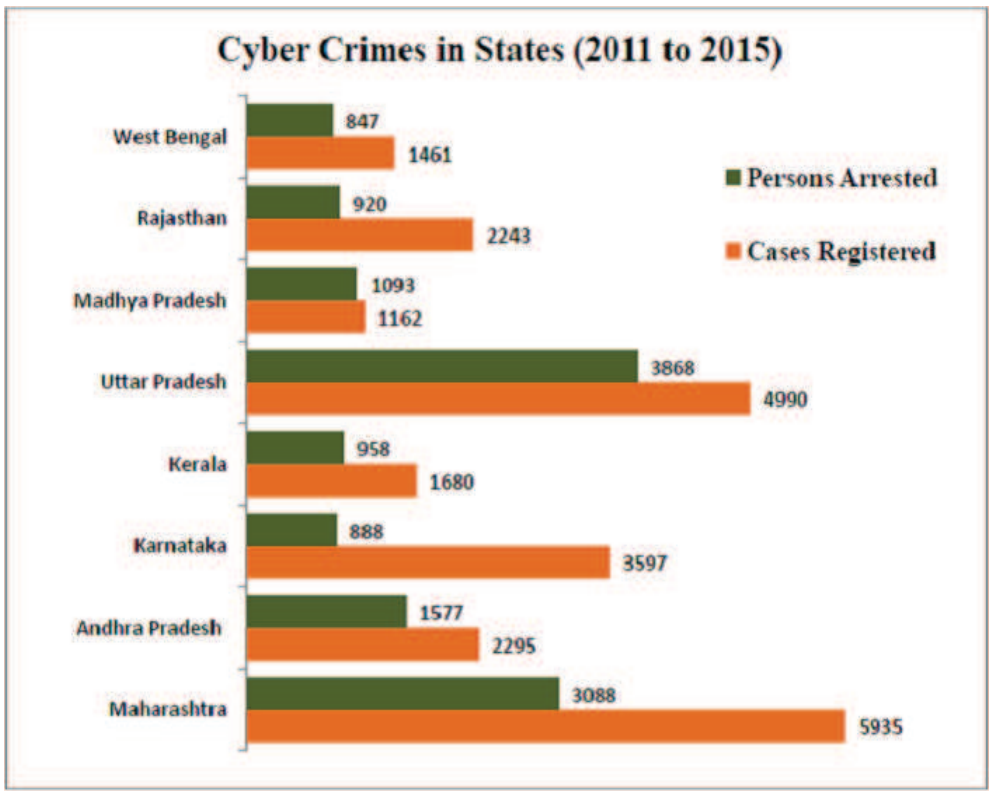
How To Prevent Hacking?:

1. Harden your systems or lock down by
   - Configuring necessary software for better security.
   - Uninstalling unnecessary software – remove any daemons that aren't needed or seldom used, as they're the most vulnerable to attacks.
   - Configuring the base operating system for increased security.

Figure 1. Total cost of cyber crime in seven countries
Cost expressed in US dollars (000,000), n = 252 separate companies



* Results were not available for all fiscal years



2. Update all the systems – Intruders can gain root access through the vulnerabilities (or "holes") in your programs so keep track of "patches" and/or new versions of all the programs that you use (once the security hole is found, manufacturers usually offer patches and fixes quickly before anyone can take advantage of the holes to any large extent), and avoiding using new applications or those with previously documented vulnerabilities.
3. Install a firewall on the system, or at least on the network – Firewalls refer to either software (ex.

Zone Alarm) and/or hardware (ex. Symantec-Axent's Firewall/VPN 100 Appliance) that block network traffic coming to and leaving a system, and give permission to transmit and receive only to user-authorized software. They work at the packet level and can not only detect scan attempts but also block them.

4. Assess your network security and degree of exposure to the Internet. You can do this by following the suggestions made by EPLS.
5. Also, more complex security checks will show whether your system is exposed through uncontrolled Internet Control Message Protocol (ICMP) packets or if it can be controlled as part of DDoS slaves through ICMP.
6. When using passwords don't use
   * Real words or combinations thereof
   * numbers of significance (example, birthdates)
   * similar/same password for all your accounts
7. Use encrypted connections – encryption between client and server requires that both ends support the encryption method
   * don't use Telnet ,POP, or FTP programs unless strongly encrypted passwords are passed over the Internet; encrypt remote shell sessions (like Telnet)if switching to other user IDs/root ID
   * use SSH (instead of Telnet or FTP)
   * never send sensitive information over email
8. Do not install software from little known sites – as these programs can hide "Trojans"; if you have to download a program, use a checksum, typically PGP or MD5 encoded, to verify its authenticity prior to installation
9. Limit access to your server(s) – limit other users to certain areas of the file system or what applications they can run
10. Stop using systems that have already been compromised by hackers – reformat the hard disk(s) and re-install the operating system
11. Use Anti-Virus Software (ex. Norton Anti-Virus or MacAfee) and keep your virus definitions up-to-date. Also, scan your system regularly for viruses.
12. The government should enforce more strict laws and the judiciary should make sure that it won't allow any of the hacker to escape from punishment. Only when the law is enforced then only that law has some meaning. There is a need for dedicated, continuous, updated training of the law enforcement agencies. There is also a lack of dedicated cybercrime courts in the country where expertise in cybercrime can be utilized. Initiative has to come from Law Enforcement Agencies to make systematic effort in imparting training to prosecutors and judges.
13. Most important of all is that people must be aware of it. As popularly said in Indian constitution, "Ignorance of law is not an excuse", in the same manner it is up to the people. Update them regarding the new laws and learn to protect them from being hacked or be a victim of any form of Cyber crime.

References:

1. Kauser Husain, "Cyber Crime against Children-A new threat to the society".
2. LawZ Bureau, "Are You Secure?"
3. Arpan Das Gupta, Dr. Madhumita Roy, Probable Variables Of Transition Of Built Forms.; Engineering Sciences international Research Journal : ISSN 2320-4338 Volume 3 Issue 2 (2015), Pg 26-32
4. M. P. Jain – Constitution of India
5. NationalLawJournal-www.nationallawjournal.com
6. National Cyber Security System
7. https://en.wikipedia.org/wiki/Hacker
8. Teesha Majumder, Enabling And Creating Supportive Design Model For Elderly And Orphans – A Sustainable Approach.; Engineering Sciences international Research Journal : ISSN 2320-4338 Volume 3 Issue 2 (2015), Pg 33-37
9. http://www.crucialp.com/resources/tutorials/website-web-page-site-optimization/hacking-attacks-prevention/

Akhil Bhusanur
Student, #35, GF, 1st Cross, GKW Layout, Vijaynagar, Bangalore -560040.
Akhila Wali
Student, #20, Above SBM Building, Adarsh Nagar, Hubli -580032.