International Journal of Basic and Applied Sciences Vol. 2. No. 4. 2013. Pp. 150-156

Full Length Research Paper

Latest Face of Cybercrime and Its Prevention In India

***Vineet Kandpal and **R. K. Singh**

** MCA Student, IGNOU, New Delhi.*

*** Scientist-D (Information Technology), G. B. Pant Institute of Himalayan Environment and Development, Kosi- Katarmal, Almora – 263643, Uttarakhand, India.*

****Corresponding author: Vineet Kandpal***

Abstract

The Internet is a global system of interconnected computer networks that use the standard Internet Protocol Suite (TCP/IP) to serve billions of users worldwide. The Internet carries a vast range of information resources and services, such as the inter-linked hypertext documents of the World Wide Web (WWW) and the infrastructure to support electronic mail. Through internet and WWW, any one can access information at any time and any where but the data which is available online can be targeted by third person in a way of hacking, pishing, etc. to harm the computer and information stored in computer or available online. This type of happening is called cyber crime. Cyber crime always involves some degree of infringement on the privacy of others or damage to computer-based property such as files, web pages or software. This paper is completely focused on cyber crime issue, trends and problem faced by Indian users and how cyber crimes can be minimized by formulating effective cyber crime laws in India. The paper also includes Indian cybercrime Statistics, cyber crime cells all over India and many more latest news. National level agencies can develop security guidelines and policy to prevent and safeguard of internet users from cyber crimes.

Keywords: *Internet, WWW, Cyber world, Cyber crime, Hacking, Cyber laws, Indian cybercrime Statistics, Cyber cells in India*

Introduction

These days computer and internet becomes very common and necessary for our daily life. Back in 1990, less than 1,00,000 people were able access Internet worldwide. Now around 2,405,518,376 people are hooked up to surf the net around the globe. The present time of fast computing brings a new world known as cyber world. The increasing use of information technology facilitate common people to get information, store information, share information etc. The cyber world is an online world where users have a lot of information technology mechanisms to do personal activity as easily and freely as they can transact them in the physical world.

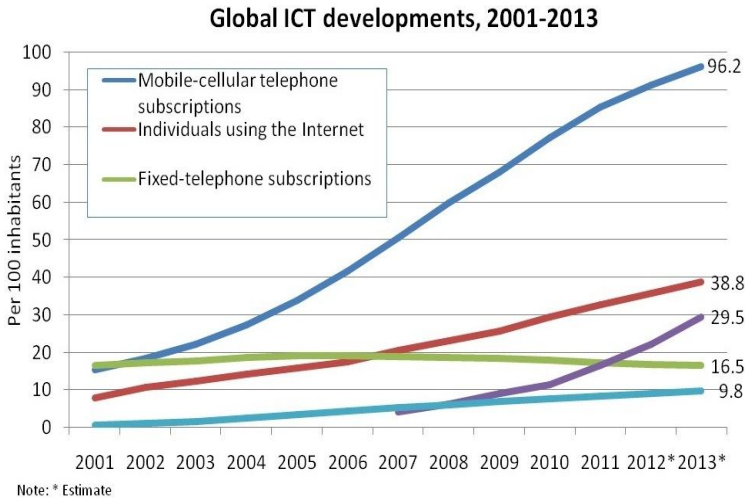

Fig.1. Trend of global ICT development (2001-2013)
(Source: http://www.itu.int/en/ITUD/Statistics/Pages/stat/default.aspx)

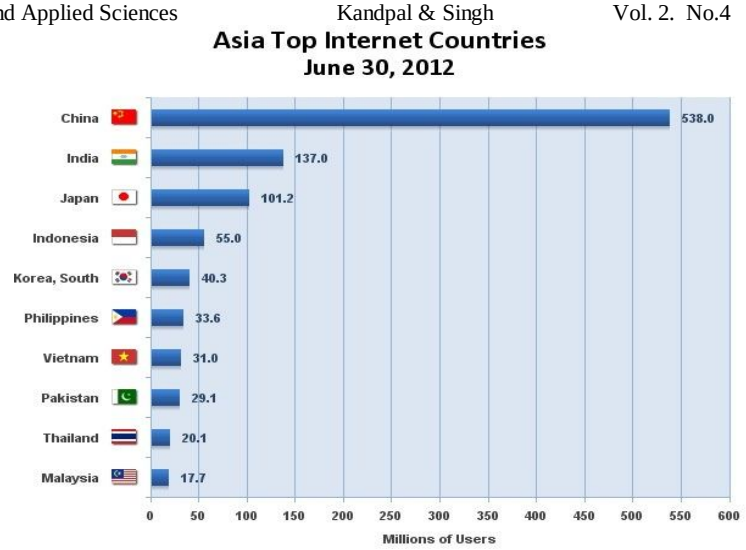

Fig.2. County wise use of internt facility
(Source: http://www.internetworldstats.com/stats3.htm)

Internet and World Wide Web works as a backbone for all online service and activities. Users can access these online services at anytime and from any where. Internet offers great benefit to society but present opportunities for crime also. Today e-mail and websites have become the preferred means of data communication. This includes not only educational and informative material but also information that might be personal.

What is Cyber Crime?

As the use of internet is increasing, a new face of crime is spreading rapidly from in-person crime to nameless and faceless crimes involving computers. Cyber crime includes all unauthorized access of information and break security like privacy, password, etc. with the use of internet. Cyber crimes also includes criminal activities performed by the use of computers like virus attacks, financial crimes, sale of illegal articles, pornography, online gambling, e-mail spamming, cyber phishing, cyber stalking, unauthorized access to computer system, theft of information contained in the electronic form, e-mail bombing, physically damaging the computer system, etc.

In tenth United Nations congress on "prevention of crime and treatment of offenders" which is devoted to issues of crimes related to computer networks, cyber crime was broken into two categories and defined as:

***a. Cyber crime in a narrow sense (computer crime*):** Any illegal behavior directed by means of electronic operations that targets the security of computer systems and the data processed by them.

b. Cyber crime in a broader sense (computer-related crime): Any illegal behavior committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and offering or distributing information by means of a computer system or network.

Cyber Crime Includes

Following are the few examples of cyber crime:

- ***Cyber stalking:*** Online harassment and online abuse all comes under stalking. It generally involves harassing or threatening behavior that an individual engages in repeatedly, such as following a person, appearing at a person's home or place of business, making harassing phone calls, leaving written messages or objects, or vandalizing a person's property. Cyber stalking shares important characteristics with offline stalking; many stalkers (online or off) are motivated by a desire to control their victims. A major damaging effect of online abuse is a victim avoiding his/her friends, family and social activities.

- ***Intellectual Property Crimes:*** Intellectual property consists of a bundle of rights. Any unlawful act by which the owner is deprived completely or partially of his rights is an offence. The common form of IPR violation may be said to be software piracy, infringement of copyright, trademark, patents, designs and service mark violation, theft of computer source code, etc.

- ***Bot Networks:*** The word botnet made from the two words robot and network. A cyber crime called 'Bot Networks', when hackers remotely take control upon computers by using malware software. Computers can be co-opted into a botnet when they execute malicious software. A botnet's originator can control the group remotely.

- ***Transmitting Virus:*** Viruses are programs that attach themselves to a computer or a file and then circulate themselves to other files and to other computers on a network. They usually affect the data on a computer, either by altering or deleting it. Worm attacks plays major role in affecting the computerize system of the individuals.

- ***Hacking:*** In general words hacking means seeking and exploiting weakness and security of a computer system or a computer network for unauthorized access. The person who do hacking is known as hacker. Hacker use computer expertise and some tool or scripts to hack any computer system.

- ***Internet Time Thefts:*** Basically, Internet time theft comes under hacking. It is the use by an unauthorized person, of the Internet hours paid for by another person. The person who gets access to someone else's ISP user ID and password, either by hacking or by gaining access to it by illegal means, uses it to access the Internet without the other person's knowledge.

- ***Cracking:*** It is a dreadful feeling to know that a stranger has broken into user computer systems without user's knowledge and consent and has tampered with precious confidential data and information. Cracker are differ with hacker because hacker are hired by companies to audit network security or test software but cracker do same work for their own profit or to harm others.

- ***Phishing:*** Phishing means acquire information such as usernames, passwords, credit card details, personal detail etc by electronic communication. Phishing commonly uses fake emails or fake messages which contain link of virus/ malware infected fake websites. These website request user to enter their personal detail.

- ***Voice Phishing:*** The term is a combination of "voice" and phishing. Voice phishing is use to gain access of private, personal and financial information from the public. Voice phishing uses a landline telephone call to get information.

- **Carding:** It means false ATM cards i.e. Debit and Credit cards used by criminals for their monetary benefits through withdrawing money from the victim's bank account.

- ***E-Mail/SMS Spoofing:*** A spoofed E-mail/ SMS may be said to be one, which misrepresents its origin. It shows it's origin to be different from which actually it originates. Here an offender steals identity of another in the form of email address, mobile phone number etc and send message via internet.

- ***Cross-site Scripting:*** Cross-site scripting (XSS) is a type of computer security vulnerability. By cross-site scripting attacker can bypass the predefine access permissions of website. Reflected XSS is the most frequent type of XSS attack. Reflected XSS attack is also known as non-persistent XSS. Scripting languages like java script, VBScript etc are use for Reflected XSS attack.

- ***Cyber Squatting:*** Squatting is the act of occupying an abandoned or unoccupied space. Cyber squatting is the act of registering a famous domain name and then selling it to needy in high cost. It means where two persons claim for the same Domain Name either by claiming that they had registered the name first on by right of using it before the other or using something similar to that previously.

- ***Child Pornography:*** It involves the use of computer networks to create, distribute, or access materials that sexually exploit underage children. Child pornography is divided into *simulated child pornography* and *pornography* which was produced with direct involvement of the child (also known as child abuse images).

- ***Cyber Vandalism:*** Vandalism means destroying or damaging property of another. Thus cyber vandalism means destroying or damaging the data when a network service is stopped or disrupted. It may include within its purview any kind of physical harm done to the computer of any person.

- ***Cyber Trespass:*** It means to access someone's computer without the right authorization of the owner and does not disturb, alter, misuse, or damage data or system by using wireless internet connection.

- ***Cyber Trafficking:*** It may be trafficking in drugs, human beings, arms weapons etc. which affects large number of persons. Trafficking in the cyberspace is also a gravest crime.

- ***Cyber crime & Social Networking:*** Cyber criminals use social media not only to commit crime online, but also for carrying out real world crime owing to "over-sharing" across these social platforms**.** The risk associated with our identities. Identity theft can happen to anyone who exposes too much personal information online on various social networking sites. Get to know the security and privacy settings, and configure them to protect from identity theft. One in five online adults (21 percent) has reported of becoming a victim of either social or mobile cyber crime and 39 percent of social network users have been victims of profile hacking, scam or fake link.

Present Trends of Cyber Crime in India

In the case of cyber crime, large numbers of suitable targets may emerge through increasing time spent online, and the use of online services such as banking, shopping and file sharing making users prone to phishing attacks or fraud. The major cyber crimes reported in India are denial of web services, hacking of websites, computer virus and worms, pornography, cyber squatting, cyber stalking and phishing. Nearly 69 percent of information theft is carried out by current and ex-employees and 31 per cent by hackers. India has to go a long way in protecting the vital information.

According to Symantec's (American Global Computer Security Software Corporation) internet security threat report (volume 18) on April 29, 2013, India has seen a 280 percent increase in bot infections that is continuing to spread to a larger number of emerging cities in India. India has the highest ratio in the world of outgoing spam or junk mail of around 280 million per day worldwide. India's home PC owners are the most targeted sector of cyber attacks. Mumbai and Delhi emerging as the top two cities for cyber crime.

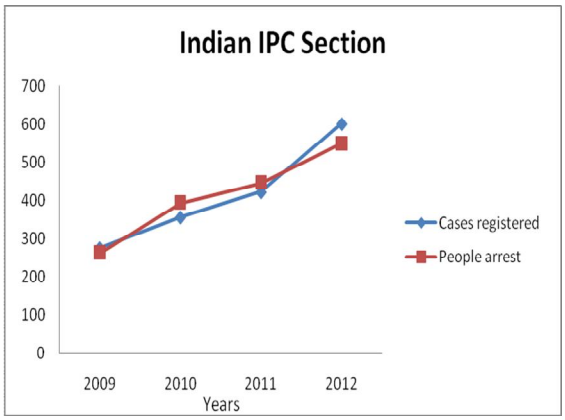

Fig.3. Case registered under Indian IPC section

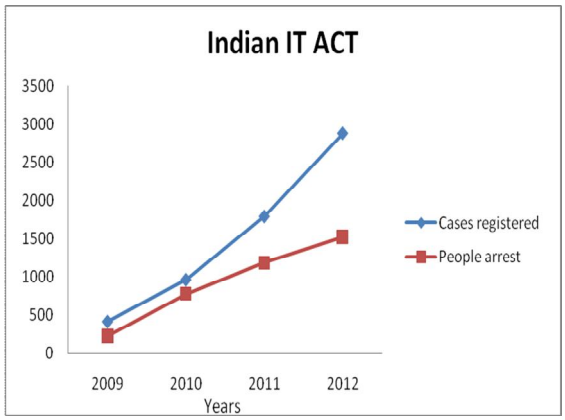

Fig.4. Case registered under Indian IT Act

(Source: Crime in India- 2012, Compendium, National Crime Records Bureau Ministry of Home Affairs Government of India)

Incidence of Cyber Crimes (IT Act + IPC Sections) has increased by 57.1% in 2012 as compared to 2011 (from 2,213 in 2011 to 3,477 in 2012). Cyber Fraud accounted for 46.9% (282 out of 601) and Cyber Forgery accounted for 43.1% (259 out of total 601) were the main cases under IPC category for Cyber Crimes. 61.0% of the offenders under IT Act were in the age group 18-30 years (928 out of 1,522) and 45.2% of the offenders under IPC Sections were also in the age group 18-30 years (248 out of 549).

According to Indian Ministry of Communications & Information Technology, around 78 government websites were hacked and 16,035 security incidents related to scanning, spam, malware infection, denial of service and system break-in including that of Government, Defense and public sector undertakings were reported up to June, 2013. The number of security breach incidents stood at 13,301 in 2011 and 22,060 in 2012. According to Indian Computer Response Team (CERT-In) a total number of 308, 371 and 78 government websites were hacked during the years 2011, 2012 and 2013 (up to June).

Table-1: Statistics of case registered and people arrested under Indian IPC Section and IT Act

Year	Under Indian IPC Sections		Under Indian IT ACT	
	Cases registered	People arrest	Cases registered	People arrest
2009	276	263	420	228
2010	356	394	966	779
2011	422	446	1791	1184
2012	601	549	2876	1522

(Source: Crime in India- 2012, Compendium, National Crime Records Bureau Ministry of Home Affairs Government of India)

Cyber Laws in India

Cyber law was first step taken by Governent to stop cybercrime. According to indian law cyber crime has to be voluntary and willful, an act or omission that adversely affects a person or property. Cyber law encompasses laws relating to Cyber Crimes, Electronic and Digital Signatures, Intellectual Property, Data Protection and Privacy. Indian parliament passed its first "*Information Technology Act, 2000*" on 17th October 2000 to deal with cybercrime in the field of e-commerce, e-governance, e-banking as well as penalties and punishments. The Information Technology (IT) Act, 2000, specifies the acts which have been made punishable.

On 17th October 2000 the Information Technology (Certifying Authorities) Rules, 2000 and Cyber Regulations Appellate Tribunal (Procedure) Rules, 2000 came into force. On 17th March 2003, the Information Technology (Qualification and Experience of Adjudicating Officers and Manner of Holding Enquiry) Rules, 2003 were passed. The Information Technology

(Security Procedure) Rules, 2004 came into force on 29th October 2004. They prescribe provisions relating to secure digital signatures and secure electronic records. An important order relating to blocking of websites was passed on 27th February, 2003. According to which, Computer Emergency Response Team (CERT-IND) can instruct Department of Telecommunications (DOT) to block a website.

The Indian Penal Code (as amended by the IT Act) penalizes several cyber crimes. These include forgery of electronic records, cyber frauds, destroying electronic evidence etc. Digital Evidence is to be collected and proven in court as per the provisions of the Indian Evidence Act (as amended by the IT Act). In case of bank records, the provisions of the Bankers' Book Evidence Act (as amended by the IT Act) are relevant. Investigation and adjudication of cyber crimes is done in accordance with the provisions of the Code of Criminal Procedure and the IT Act. The Reserve Bank of India Act was also amended by the IT Act.

Penalty for Damage to Computer System

According to the Section: 43 of 'Information Technology Act, 2000' whoever does any act of destroys, deletes, alters and disrupts or causes disruption of any computer with the intention of damaging of the whole data of the computer system without the permission of the owner of the computer, shall be punishable. According to the Section:43A which is inserted by 'Information Technology(Amendment) Act, 2008' where a body corporate is maintaining and protecting the data of the persons as provided by the central government, if there is any negligent act or failure in protecting the data/ information then a body corporate shall be liable to pay compensation to person so affected. Section 66 deals with 'hacking with computer system' and provides for imprisonment up to 3 years or fine, which may extend up to 2 years or both.

Best Practices for Prevention of Cyber Crime

Below mentioned security guidelines and good practices may be followed to minimize the security risk of Cyber crime:

- ***By updating the computer:*** To avoid cyber attacks, regularly update operating system of computers and antivirus. While keeping computer up to date will not protect user from all attacks, it makes it much more difficult for hackers to access computer system, blocks many basic and automated attacks completely etc.

- ***By choosing strong passwords:*** Passwords are online identity over internet. Always select a password that have at least eight characters and use a combination of letters, numbers, and symbols (e.g. # $ % ! ?). Avoid using easy password like name, city name etc. use non dictionary words. Keep passwords in safe place and not use same password for every online service. Change passwords on a regular basis, at least every 90 days.

- ***By protecting computer with security software:*** Security software commonly includes firewall and antivirus programs. A firewall controls who and what can communicate with computer online. Antivirus software monitors all online activities and protects computer from viruses, worms, Trojan horses, and other types of malicious programs. Antivirus and antispyware software should be configured to update itself, and it should do so every time connect to the Internet.

- ***Shield personal information:*** To take advantage of many online services, users will have to provide personal information in order to handle billing and shipping of purchased goods. The following list contains some advice for how to share personal information safely online:
  - Phishing messages will often tell that to act quickly to keep account open, update security, or else something bad will happen. Don't respond them.
  - Don't respond to email messages that ask for personal information. True companies will not use email messages to ask for personal information.
  - When visiting a website, type the URL directly into the Web browser rather than follow a link within an email or instant message.
  - Guard email address from unwanted emails.

- ***Online offers that look too good to be true usually are:*** The free software or service asked for may have been bundled with advertising stuff that tracks behavior and displays unwanted advertisements. Be careful while downloading free stuff.

- ***Review bank and credit card statements regularly:*** The impact of identity theft and online crimes can be greatly reduced if user can catch it shortly after their data is stolen or when user gets symptoms. Regularly check bank and credit card's statements. Now, many banks and services use fraud prevention systems that call out unusual purchasing behavior.

- ***Be Social-Media Savvy:*** Make sure social networking profiles (e.g. Facebook, Twitter, etc.) are set to private. Check security settings with in frequent intervals. Be careful what information post online.

- ***Secure Mobile Devices:*** Be aware that mobile device is vulnerable to viruses and hackers. Download applications from trusted sources.

- ***Secure wireless network:*** Wi-Fi (wireless) networks at home are vulnerable to intrusion if they are not properly secured. Review and modify default settings. Avoid using public WiFi spots.

- ***Call the right person for help:*** If computer crime is suspected by a way of identity theft or a commercial scam then immediately report this to local police. If help is needed for maintenance or software installations on computer then consult with authenticated service provider or a certified computer technician.

Cyber Crime Cells in India

To solve cyber crime cases, Indian police developed cyber crime investigation cells all over India. These Cyber Crime cell investigates in respect of cases pertaining to hacking, spread of virus, pornography, manipulation of accounts, alteration of data, software piracy, creation of false Web sites, printing of counterfeit currency, forged visas, theft of intellectual property, email spamming, denial of access, password theft, crimes with cell phones and palmtops, cyber terrorism etc.. The following table shows the phone numbers and email address of few cyber crime cells operational in India:

Table-2: List of cyber crime cells all over India.

Assam - CID HQ,Dy.SP. Ph: +91-361-252-618, 9435045242 E-mail: ssp_cod@assampolice.com	**Chennai** - Assistant Commissioner of Police Ph: +91-40-5549 8211 E-mail id: s.balu@nic.in
Bangalore - Cyber Crime Police Station Ph: +91-80-2220 1026, 91-80-2294 3050 Email: ccps@blr.vsnl.net.in, ccps@kar.nic.in	**Hyderabad** - Cyber Crime Police Station Ph: +91-40-2324 0663, 91-40-2785 2274 Email: cidap@cidap.gov.in, info@cidap.gov.in
Delhi - CBI Cyber Crime Cell: Ph: +91-11-4362203, 91-11-4392424 Email: cbiccic@bol.net.in	**Thane** - Police Commissioner Office Ph: +91-22-25424444 Email: police@thanepolice.org
Pune- Deputy Commissioner of Police(Crime) Ph: +91-20-26123346, 91-20-26127277 E-Mail: crimecomp.pune@nic.in	**Mumbai** - Cyber Crime Investigation Cell Ph: +91-22-22630829, 91-22-22641261 Email: officer@cybercellmumbai.com
Jharkhand - IG- CID, Organized Crime Ph: +91-651-2400 737/ 738 Email: a.gupta@jharkhandpolice.gov.in	**Himachal Pradesh** - CID Office , Ph: +91-94180 39449 Email:soodbrijesh9@gmail.com
Haryana Joint Commissioner of Police Email: jtcp.ggn@hry.nic.in	**Gujarat** - DIG, CID, Crime and Railways Ph: +91-79-2325 4384, 91-79-2325 0798
Jammu - SSP,Crime Ph: +91-191-257-8901 Email: sspcrmjmu-jk@nic.in	**Kerala** - Hitech Cell, Police Head Quarters Ph: +91-471 272 1547, 91-471 272 2768 Email: hitechcell@keralapolice.gov.in
Meghalaya - SCRB, Superintendent of Police Ph: +91 98630 64997 Email: scrb-meg@nic.in	**Orissa** - CID, Crime Branch Ph: +91 94374 50370 Email: splcidcb.orpol@nic.in
Bihar - Cyber Crime Investigation Unit Ph: +91 94318 18398, Email: cciu-bih@nic.in	**Punjab** - Cyber Crime Police Station Ph: +91 172 2748 100
Uttar Pradesh - Cyber Complaints Redressal Cell, Ph:919410837559 Email: info@cybercellagra.com	**West Bengal** - CID, Cyber Crime Ph: +9133 24506163 Email: occyber@cidwestbengal.gov.in
Uttarakhand - Special Task Force Office Ph: +91 135 2640982, 91 94123 70272 Email: dgc-police-us@nic.in	

(Source: http://infosecawareness.in/cyber-crime-cells-in-india)

Conclusion

At present criminals have changed their method and have started using advanced technology. In order to deal with them the society, the legal and law enforcement authorities will also have to change. All cyber crime is based on lack of awareness. This is a duty of Government, print media to educate unwary persons about the dangerous areas of the cyber-world because prevention is better than cure. Cyber Space Security Management has already become an important component of National Security Management, Military Security Management, Scientific Security Management and Intelligence Management all over the world. Yet India has taken a lot of steps to stop cyber crime but the cyber law cannot afford to be static, it has to change with the changing time.

References

Crime in India: 2011-Compendium (2012), National Crime Records Bureau, Ministry of Home Affairs, Government of India, New Delhi, India.

Cyber Law & Information Technology (2011) by Talwant Singh, Additional District & Sessions Judge, New Delhi, India.

Introduction to Indian Cyber Law (2008) by Rohas Nagpal, Asian School of Cyber Laws, Pune, India

Cyber Crime (2003) by R.K. Suri and T.N. Chhabra, Pentagon Press, New Delhi, India.

Cyber Laws in the Information Technology Age (2009) by Karnika Seth, Jain Book Depot, New Delhi, India.
Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives (2012) by Nina Godbole and Sunil Belapure, Wiley India Pvt. Ltd, New Delhi, India.
Cyber Crime and the Victimization of Women: Laws, Rights and Regulations (2011) by Debarati Haldaer (Centre for Cyber Victim Counseling, India) and K. Jaishankar (Manonmaniam Sundaranar University, India), IGI Global, USA.
http://www.philstar.com/business/2013/03/12/918801/study-social-networks-new-haven-cybercrime
http://www.symantec.com/en/in/about/news/release/article.jsp?prid=20130428_01
http://www.internetworldstats.com/stats.htm
http://en.wikipedia.org/wiki/Computer_crime