TECHNOLOGY FACTORY

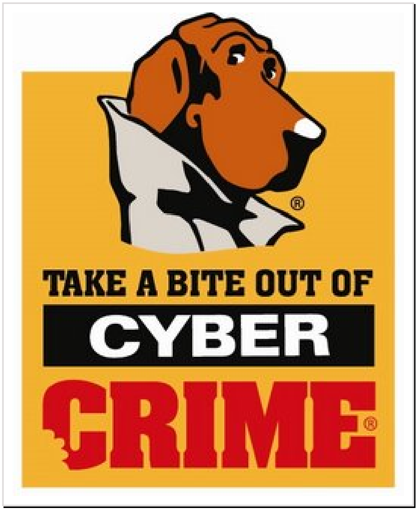
FIRST CHOICE FOR YOUR TECHNO-LIFE!

HOME | Computer | Android | Apple | Internet And Cyber | Internet And Marketing | Laptop | Technology | Web Design | Scientific Facts In The Quran | Blog

http://technologyfactory.blogspot.com/ » Internet and cyber » Do You Know Cyber Crime ?

Do You Know Cyber Crime ?

Written By technology factory on Wednesday, 7 December 2011 | 14:15



The internet in India is growing rapidly. It has given rise to new opportunities in every field we can think of – be it entertainment, business, sports or education. There are two sides to a coin. Internet also has its own disadvantages. One of the major disadvantages is Cybercrime – illegal activitiy committed on the internet. The internet, along with its advantages, has also exposed us to security risks that come with connecting to a large network. Computers today are being misused for illegal activities like e-mail espionage

, credit card fraud, spams, software piracy and so on, which invade our privacy and offend our senses. Criminal activities in the cyberspace are on the rise. Here we publish an article by Nandini Ramprasad in series for the benefit of our netizens. – Ed.

"The modern thief can steal more with a computer than with a gun. Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb".

– National Research Council, "Computers at Risk", 1991.

What is this Cyber crime? We read about it in newspapers very often. Let's look at the dictionary definition of Cybercrime: "It is a criminal activity committed on the internet. This is a broad term that describes everything from electronic cracking to denial of service attacks that cause electronic commerce sites to lose money".

Mr. Pavan Duggal, who is the President of cyberlaws.net and consultant, in a report has clearly defined the various categories and types of cybercrimes.

Cybercrimes can be basically divided into 3 major categories:

1. Cybercrimes against persons.

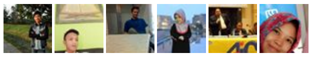
2. Cybercrimes against property.

3. Cybercrimes against government.

Cybercrimes committed against persons include various crimes like transmission of child-pornography, harassment of any one with the use of a computer such as e-mail. The trafficking, distribution, posting, and dissemination of obscene material including pornography and indecent exposure, constitutes one of the most important Cybercrimes known today. The potential harm of such a crime to humanity can

LABELS

android OS (17)
Apple (5)
Bad food (2)
business article (2)
computer (8)
history (2)
Internet and cyber (6)
internet marketing (3)
laptop (2)
Learning English (2)
listening (english) (1)
making food (6)
Scientific Facts in The Quran (12)
technology (29)
tenses (12)
water (3)
weapon (1)
web design (1)
women's health (9)



hardly be amplified. This is one Cybercrime which threatens to undermine the growth of the younger generation as also leave irreparable scars and injury on the younger generation, if not controlled.

A minor girl in Ahmedabad was lured to a private place through cyberchat by a man, who, along with his friends, attempted to gangrape her. As some passersby heard her cry, she was rescued.

Another example wherein the damage was not done to a person but to the masses is the case of the Melissa virus. The Melissa virus first appeared on the internet in March of 1999. It spread rapidly throughout computer systems in the United States and Europe. It is estimated that the virus caused 80 million dollars in damages to computers worldwide.

In the United States alone, the virus made its way through 1.2 million computers in one-fifth of the country's largest businesses. David Smith pleaded guilty on Dec. 9, 1999 to state and federal charges associated with his creation of the Melissa virus. There are numerous examples of such computer viruses few of them being "Melissa" and "love bug".

Cyberharassment is a distinct Cybercrime. Various kinds of harassment can and do occur in cyberspace, or through the use of cyberspace. Harassment can be sexual, racial, religious, or other. Persons perpetuating such harassment are also guilty of cybercrimes.

Cyberharassment as a crime also brings us to another related area of violation of privacy of citizens. Violation of privacy of online citizens is a Cybercrime of a grave nature. No one likes any other person invading the invaluable and extremely touchy area of his or her own privacy which the medium of internet grants to the citizen.

The second category of Cyber-crimes is that of Cybercrimes against all forms of property. These crimes include computer vandalism (destruction of others' property), transmission of harmful programmes.

A Mumbai-based upstart engineering company lost a say and much money in the business when the rival company, an industry major, stole the technical database from their computers with the help of a corporate cyberspy.

The third category of Cyber-crimes relate to Cybercrimes against Government. Cyberterrorism is one distinct kind of crime in this category. The growth of internet has shown that the medium of Cyberspace is being used by individuals and groups to threaten the international governments as also to terrorise the citizens of a country. This crime manifests itself into terrorism when an individual "cracks" into a government or military maintained website.

In a report of expressindia. com, it was said that internet was becoming a boon for the terrorist organisations. According to Mr. A.K. Gupta, Deputy Director (Co-ordination), CBI, terrorist outfits are increasingly using internet to communicate and move funds. "Lashker-e-Toiba is collecting contributions online from its sympathisers all over the world. During the investigation of the Red Fort shootout in Dec. 2000, the accused Ashfaq Ahmed of this terrorist group revealed that the militants are making extensive use of the internet to communicate with the operatives and the sympathisers and also using the medium for intra-bank transfer of funds".

Cracking is amongst the gravest Cyber-crimes 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 cracking proof. It is unanimously agreed that any and every system in the world can be cracked. The recent denial of service attacks seen over the popular commercial sites like E-bay, Yahoo, Amazon and others are a new category of Cyber-crimes which are slowly emerging as being extremely dangerous.

Unauthorised access

Using one's own programming abilities as also various progra-mmes with malicious intent to gain unauthorised access to a computer or network are very serious crimes. Similarly, the creation and dissemination of harmful computer programmes 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.

Professionals who involve in these cybercrimes are called crackers and it is found that many of such professionals are still in their teens. A report written near the start of the Information Age warned that America's computers were at risk from crackers.

It said that computers that "control (our) power delivery, communications, aviation and financial services (and) store vital information, from medical re-cords to business plans, to criminal records", were vulnerable from many sources, including deliberate attack.

"Script-kiddies"

Crackers do more than just spoiling websites. Novices, who are called "script-kiddies" in their circles, gain "root" access to a computer system, giving them the same power over a system as an administrator – such as the power to modify features. They cause damage by planting viruses.

The Parliament of India passed its first Cyberlaw, the Information Technology Act in 2000. It not only provides the legal infrastructure for E-commerce in India but also at the same time, gives draconian powers to the Police to enter and search, without any warrant, any public place for the purpose of nabbing cybercriminals and preventing cybercrime. Also, the Indian Cyberlaw talks of the arrest of any person who is about to commit a cybercrime.

The Act defines five cyber-crimes – damage to computer source code, hacking, publishing electronic information whi-ch is lascivious or prurient, br-each of confidentiality and pu-blishing false digital signatu-res. The Act also specifies that cybercrimes can only be investigated by an official holding no less a rank than that of Dy. Superintendent of Police (Dy.SP).

The Act simply says "Notwi-thstanding anything contained in any other law for the time being in force, any Police Officer not below the rank of Dy.SP may enter, search and arrest any person without search warrant in any public place who he thinks is committing or about to commit a cybercrime".

It is common that many systems operators do not share information when they are victimis-ed by crackers. They don't contact law enforcement officers when their computer systems are invaded, preferring instead to fix the damage and take action to keep crackers from gaining access again with as little public attention as possible.

According to Sundari Nanda, SP, CBI, "most of the times the victims do not complain, may be because they are aware of the extent of the crime committed against them, or as in the case of business houses, they don't want to confess their system is not secure".

As the research shows, computer crime poses a real threat. Those who believe otherwise simply have not been awakened by the massive losses and setbacks experienced by companies worldwide. Money and intellectual property have been stolen, corporate operations impeded, and jobs lost as a result of computer crime.

Similarly, information systems in government and business alike have been compromised. The economic impact of computer crime is staggering.

Cyberspace

As the cases of cybercrime grows, there is a growing need to prevent them. Cyberspace belongs to everyone. There should be electronic surveillance which means investigators tracking down hackers often want to monitor a cracker as he breaks into a victim's computer system. The two basic laws governing real-time electronic surveillance in other criminal investigations also apply in this context, search warrants which means that search warrants may be obtained to gain access to the premises where the cracker is believed to have evidence of the crime. Such evidence would include the computer used to commit the crime, as well as the software used to gain unauthorised access and other evidence of the crime.

There should also be analysing evidence from a cracker's computer by the officials investigating the crime. A seized computer may be examined by a forensic computer examiner to determine what evidence of the crime exists on the computer.

Researchers must explore the problems in greater detail to learn the origins, methods, and motivations of this growing criminal group. Decision-makers in business, government, and law enforcement must react to this emerging body of knowledge. They must develop policies, methods, and regulations to detect incursions, investigate and prosecute the perpetrators, and prevent future crimes. In addition, Police Departments should immediately take steps to protect their own information systems from intrusions.

Internet provides anonymity: This is one of the reasons why criminals try to get away easily when caught and also give them a chance to commit the crime again. Therefore, we users should be careful. We should not disclose any personal information on the internet or use credit cards and if we find anything suspicious in e-mails or if the system is hacked, it should be immediately reported to the Police officials who investigate cyber-crimes rather than trying to fix the problem by ourselves.

Computer crime is a multi-billion dollar problem. Law enforcement must seek ways to keep the drawbacks from overshadowing the great promise of the computer age. Cybercrime is a menace that has to be tackled effectively not only by the official but also by the users by co-operating with the law. The founding fathers of internet wanted it to be a boon to the whole world and it is upon us to keep this tool of modernisation as a boon and not make it a bane to the society.

RELATED POST:

/Internet and cyber

- Do You Know Cyber Crime ?
- 7 Negative Effects of Facebook
- Is Google Making Us Stupid?
- Negative Effects of the Internet on Children
- Cyberbullying Types and Their Effects
- Online Identity Management Techniques

you're reading my article in my blog **Do You Know Cyber Crime ?** and you can find something Do You Know Cyber Crime ? ini dengan url **http://technologyfactory.blogspot.in/2011/12/do-you-know-cyber-crime.html**, you can publish and copy paste for you **Do You Know Cyber Crime ?** it's very use full Do You Know Cyber Crime ? sumbernya.

Tweet 0 Share 0 Email 0 Share 34

Posted by technology factory at 14:15

Labels: Internet and cyber

0 Comments

0 Comments

0 Comments Sort by Oldest ▾

Add a comment...

Facebook Comments Plugin

0 comments:

Post a Comment

dont give the spam and be polite pelase.
thank's

Enter your comment...

Comment as: Google Accou ▼

Publish Preview

Links to this post

Create a Link

Newer Post Home Older Post

Subscribe to: Post Comments (Atom)

Company Info | Contact Us | Privacy policy | Term of use | Widget | Advertise with Us | Site map

Template Design by Fajri Sabti. Published by Capt.Fajri