

VIGILANCE CIRCULAR NO. 01/2011
DATE OF ISSUE: 04.01.11

MECL, NAGPUR

Subject: Beware of Cyber Crimes.

With the increasing use of Computers for various activities of day to day life by every class and age of individuals, the cyber crimes have also started increasing manifold, affecting every individual using internet for such purposes as internet banking, payment of utility bills using credit cards etc.

Internet is not owned by any agency/organization. As such responsibility cannot be fixed on any particular organizations for the misuse of internet. However, looking at the gravity and the increasing number of crimes committed through internet, the Government has enacted IT Act 2005 to tackle the menace of Cyber crimes.

Cyber crime

Cyber Crime is where computer is the target of a crime or is the means adopted to commit a crime.

Most of these crimes are standard criminal activities such as fraud, theft, blackmail, forgery and embezzlement using Internet as the medium. Anonymity and lack of awareness of laws are the lethal weapons used by cyber criminals.

Types of Cyber crimes

E-Mail bombing: Sending a large amount of e-mails to the victim resulting in interruption in the victims' e-mail account or mail servers.

Data diddling: This kind of an attack involves altering the raw data just before it is processed by a computer and then changing it back after the processing is completed.

Salami attacks: These attacks are used for committing financial crimes. The key here is to make the alteration so insignificant that in a single case it would go completely unnoticed e.g. a bank employee inserts a program into bank's servers, that deducts an amount of ten paisa from the account of every customer every month.

Denial of Service: This involves flooding computer resources with more requests than it can handle. This causes the resources to crash thereby denying authorized users the service offered by the resources.

Phishing: Derived from the word "fishing", it means luring or enticing an unwary customer of a Banking or Financial Institution to pass on sensitive information pertaining to their account. Scammers then use this information to siphon off funds or, undertake transactions that are billed to the original customer.

Hacking: Hacking in simple terms means an illegal intrusion into a computer system and/or network.

Cyber Stalking: Cyber Stalking can be defined as the repeated acts of harassment or threatening behavior of the cyber criminal towards the victim by using internet services.

Fake Web Sites: Creation of fake websites specially of banks for the purpose of Phishing Account Numbers, Username & Passwords of net users.

E-Mail Spoofing: Spoofing means a hacker logs-in to a computer illegally using a different identity from his own.

Prevention of Cyber Crime

- Never arrange meetings with strangers.
- Don't respond to inappropriate messages or emails.
- Remember what you put online will be there forever.
- Always keep a watch on the sites that your children are accessing.
- Use only authentic address to access bank sites. (Store the address in favourites).
- Do not open unidentified e-mails/attachments.
- Remember that people online may not be who they seem to be.
- Use the latest version of a good anti-virus software package.
- Use strong passwords for internet accounts with a combination of uppercase and lowercase letters, and special characters such as !, @, # and, . Do not use easily guessable names as passwords.
- Ensure https url and the locked yellow padlock.

(UDAY BORWANKER)
CHIEF VIGILANCE OFFICER

DISTRIBUTION:

- All HODs at CHQ, Nagpur.
- All Zonal Managers
- All ROMs
-
- Copy to :
- PS to CMD
- Sr PA to D(F)
- PS to D(T)