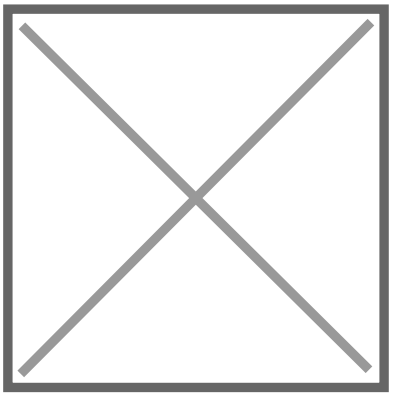

How can we deal with increasing Cyber Crimes?

Description

Background:-

- Around 11,592 cases of cyber crimes were reported across India in 2015, the number is 26 folds more than the cases reported in 2006 accounting 453 cases.
- Financial fraud and identity theft are the most common cyber crimes. A lot of people lost their hard-earned money because of cyber crimes.
- Amid Indiaâ€™s transition to cashless economy, cyber crimes are increasing multifold.

What is Cyber Crime:-

- Any crime that is committed by using computer and internet network is a cyber crime.
- In a cyber crime the computer may have been used in the commission of the crime, or it may be the target.
- Most of the cyber crimes are
    - Fraud and financial crimes
    - Cyber terrorism
    - Cyber extortion
    - Cyber warfare
    - False-flagging
    - Phishing

Causes:-

- Common people do not have much awareness on methods of cyber crimes. This is biggest advantage for criminals.
- Nonexistence of any strict laws and loopholes of the existing laws encouraging cyber crimes.
- Cyber crimes happen because there will be high rate of return on investment and the risk of loss is low.

- Financial gain was the biggest motive for cyber crimes.
- The facility of being anonymous is giving opportunity to cyber criminals.
- Cyber criminals donâ€™t have fear of rival gangs.
- Lack of digital infrastructure and network to tackle the menace.
- According to Akamai Technologies, India is among the top targets for web application attacks.

Effects:-

- Leakage of important information of vital systems such as nuclear plants, railways andhospitals that can lead to dire consequences.
- Financial frauds and fake online lottery and job scams damage the economic condition.
- Stalking, cyber bullying and harassment through online increased drastically.
- Cyber crime may cause damage to the social and communal harmony by spreading provocative media files and messages without the fear of being caught thus encouraging youth to get involved in such activities.
- It may cause big losses to the business industry by creating fake companies, transactions and deals in sales etc.

What India is doing:-

- Indian Government is spreading awareness though advertisements in televisions about fraud phone calls and cyber crimes.
- India has â€˜Information Technology Act, 2000â€™ in law.
- India has â€˜Cyber Crime police stationsâ€˜, which deal with cyber crimes exclusively.
- â€œNational Critical Information Infrastructure Protection Centerâ€• (NCIIPC) has been established as the nodal agency for the protection of critical information infrastructure.

Best practices :-

- Number of cyber security soldiers needs to be increased on a war-footing.
- Digital literacy rates should be increased, so that dependence on others for cashless transactions will be reduced. Thereby, less chances of financial fraud.
- Cyber vulnerabilities should be identified.
- Financial sector and cyber security industry should collaborate.
- People should not reveal too much personal information on the internet.

Conclusion:-

Whole world is fighting against cyber crimes. Some countries have advanced technology and human resources to deal with them. And some countries do not have that yet. India needs to increase its investment on cyber security and should spend on awareness programs on war-footing.

Afterwords :- What is your opinion on this topic? Express your thoughts in the comment section below.