National Cyber Safety and Security Standards have done an extensive research in the Cyber domain to understand the nature of cyber threats and Cyber Crimes. We have understood that the multi – faceted cyber technology cannot be handled by common standards and security policies. We came to know that, it needs different strategies for different sectors of Cyber domain.

The National Cyber Safety and Security Standards is an Autonomous Body, which is controlled and monitored by the High Level Committee Chaired by Honourable Justice Dr. S. Mohan, Former Judge, Supreme Court of India and Chairman, National Cyber Safety and Security Standards .

The Greatness of INDIA

India "Truth Alone Triumphs"(Satyameva Jayate)

Present Scrutiny

- 5,000 Years Old Ancient Civilization.
- 530 Languages Spoken.
- 652 Dialects.
- 18 Official Languages.
- 28 States, 7 Union Territories.
- 3.28 Million Sq. Kilometres - Area.
- 7,516 Kilometres - Coastline.
- 1.23 Billion Population.
- 5600 Dailies, 15000 Weeklies and 20000 Periodicals in 21 Languages with a Combined Circulation of 142 Million.
- GDP $1840 Billion. (GDP Rate 5.5%).
- Parliamentary Form of Government World's Largest Democracy.
- World's 4th Largest Economy.
- World-Class Recognition in IT, Bio-Technology and Space.
- Largest English Speaking Nation in the World.
- 3rd Largest Standing Army Force, Over 1.5 Million Strong.
- 2nd Largest Pool of Scientists and Engineers in the World.

Dedicated to Our Nation

OFFICER'S HANDBOOK ON CYBER SECURITY

NATIONAL CYBER SAFETY AND SECURITY STANDARDS
(An Autonomous Body)

"Terrorism is changing in character and expanding in its reach. Internet has made recruitment and call to violence self-generated. It also feeds off money laundering, drug trafficking and arms smuggling. We need a comprehensive global strategy for a global problem."

Shri. Narendra Modi
Honourable Prime Minister of India.

OFFICER'S HANDBOOK ON
CYBER SECURITY

[Not For Sale]

NATIONAL CYBER SAFETY AND SECURITY STANDARDS

(An Autonomous Body)

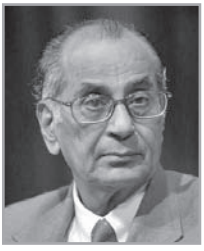
OFFICER'S HANDBOOK ON CYBER SECURITY

NATIONAL CYBER SAFETY AND SECURITY STANDARDS

Published by the Office of the Additional Director – General
Publication Division
National Cyber Safety and Security Standards
(An Autonomous Body)

CYBER HOUSE – Southern Region
No: 1, 1st Floor, 1st Avenue,
8th Cross Street, Indira Nagar Main Road,
Adyar, Chennai – 600020.

Phone : 044 – 2440 1766 / 044 – 2445 1766
Fax : 084688 65111
Email : support @nationalcybersafety.com
Website : www.ncdrc.res.in



Honourable Dr. Justice S. Mohan
Former Judge, Supreme Court of India
Chairman – National Cyber Safety and Security Standards

Foreword

Today the cyber world has come to occupy an important place in the history of mankind. As science advances, the knowledge also expands. It is undeniable fact that cyber world has thrown a new vista but regretfully it has to be noted that it has also being misused and spreading undesirable information. It has become necessary to find out ways and means to curb this menace of spreading evil knowledge

We live in the electronics age in which every institution of Government, Business and Industry, big and small, and even the family interact and communicate with one another electronically. Electronic devices which process data are no longer confined to what we traditionally consider as

computers, but are pervasive in everyday life. They range from mobile 'smart' telephones to global positioning by satellite devices, and from health-monitoring devices to defibrillators.

Information Security is an art, not a science and the mastery of information security requires a multi-disciplinary knowledge of huge quantity of information, experience, and skill. There is a great satisfaction knowing that your employer's information, communications, systems, and people are secure. Comprehensiveness is an important part of the game you play for real stakes because the enemy will likely seek the easiest way to attacks the vulnerabilities and assets that you haven't fully protected yet.

The past decade has witnessed tremendous legal reform by countries around the world. The most influential-electronic commerce has led countries to revise and update their rules of evidence on the proof and admissibility of such evidence. And litigants have responded courts are witnessing a myriad and a rising volume of electronic evidence tendered by the parties. These ranges from emails to mobile messages, from chat records to blog entries and even "tweets" to mobile messages, resolving the many difficult issues regarding discovery and inspection of electronic documents (or electronically stores information) and the

authentication and admission of electronic evidence now calls for a technologically savvy bar.

The book entitled, Cyber Crime, Types of Cyber Crime and Tips on Protecting Yourself against Cyber Crime, Computer Viruses and Solutions to Computer Viruses, Online Fraud and Financial Transactions and Instructions on Protecting Yourself against Cyber Crime, Cyber War and Cyber Terrorism and Ways on How to Prevent Cyber Terrorism from Happening.

I am glad to note that National Cyber Safety and Security Standards is publishing an Officer's Handbook on Cyber Security. This book is very useful to all the people who are working in the Government Sector. I convey my best wishes to the National Cyber Safety and Security Standards publishing committee.

Dr. S. Amar Prasad Reddy
Additional Director – General
National Cyber Safety and Security Standards

Preface

Today, the internet has turned 40, and with its maturing, the threats are increasing. Botnets and cyber-criminals are making news regularly. It has become increasingly obvious to everybody that something needs to be done to secure not only our nation's critical infrastructure but also the businesses we deal with on daily basis. The question is, "where do we begin?" what can the average information technology professional do to secure the systems that he or she is hired to maintain? One immediate answer is education and training. If we want to secure our computer systems and networks, we need to know how to do this and what security entails.

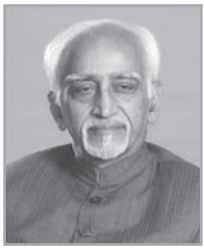
As global networks expand the interconnection of the world's information systems, the smooth operation of communication and computing solutions becomes vital.

However, recurring events such as virus and worm attacks and the success of criminal attackers illustrate the weaknesses in current information technologies and the need to provide heightened security for these systems.

In the contemporary times, when the business of Government and public sector undertakings is conducted on-line, there is always looming threat of invasion/hacking by criminals and anti-national elements. These initiatives from National Cyber Safety and Security Standards has provided insight into the techniques which can frustrate and preempt such attempts. The work of this nature elevates the standards to safeguard website from invasion and intrusion, by miscreants and it also immaculately spells out the prescription for detection of cyber crime.

The Cyber World has been created by computers and computer networks. Internet, an electronic communication network, which connects all computer networks around the world, is an interactive tool for instant access of information and knowledge on any subject. The web has created the super express highway of communication and infotainment connecting every part of the globe which, in turn, has made the concept of Global Village a virtual reality.

I wish, the Initiatives of National Cyber Safety and Security Standards plays a vital role, in the mission of building a secure and resilient cyberspace for citizens, business and Government.



His Excellency Mohammad Hamid Ansari

The Vice President of India

Honorable Vice President of India is happy to know that, National Cyber Safety & Security Standards is focusing on the issues of cyber crime in our country.

The Vice President of India extends his greetings and good wishes to the National Cyber Safety & Security Standards.

Shri. Narendra Modi
Honourable Prime Minister of India

I hope the Handbook will establish and convey the most effective ways and means of protecting our national security against the worst sort of cyber attacks and provide the best safe guards against the cyber criminals threatening our Nation and its integrity.

I wish all the success to the National Cyber Safety and Security Standards in its crusade to protect the Nation.

Institutional Partners

- Ministry of Commerce and Industry, Government of India.
- Ministry of Social Justice and Empowerment, Government of India.
- Ministry of Micro, Small and Medium Enterprises (MSME), Government of India.
- All India Council for Technical Education (AICTE).
- Government of Andhra Pradesh.
- Government of Goa.
- Government of Manipur.
- Government of Karnataka.
- Government of Madhya Pradesh.
- Government of Maharashtra.
- Gauhati High Court.
- Chandigarh Judicial Academy.
- Odisha Judicial Academy, Cuttack.
- Department of Science & Technology, Government of Gujarat.
- Central Bureau of Investigation, Anti-Corruption Branch, Chandigarh.
- Central Bureau of Investigation/Anti-Corruption

Branch, Jabalpur, Madhya Pradesh.

- Police Headquarters, Andaman & Nicobar Islands.
- Central Bureau of Investigation, Anti-Corruption Branch, Chennai, Tamil Nadu.
- Central Bureau of Investigation, Shimla, Himachal Pradesh.
- Central Bureau of Investigation, Anti-Corruption Branch, Ghaziabad, Uttar Pradesh.
- Crime Investigation Department, Andhra Pradesh.
- Central Bureau of Investigation, Mumbai.
- Central Bureau of Investigation, Anti-Corruption Branch, Patna, Bihar.
- Assam Police.
- Gujarat Police.
- Maharashtra Police.
- Uttar Pradesh Police.
- National Law University, Delhi.
- Police Training College, Daroh, Himachal Pradesh.
- Punjab Police Academy, Jalandhar.
- Police Radio Training School, Indore, Madhya Pradesh.

National Cyber Safety and Security Standards

National Cyber Safety and Security Standards have been started with great vision to safeguard the Nation from the current threats in the Cyber Space. The multi-dimensional structure of technology in the Cyberspace poses a great challenge in handling the complex problems in the Cyber Domain.

National Cyber Safety and Security Standards have done an extensive research in the Cyber domain to understand the nature of cyber threats and Cyber Crimes. We have understood that the multi-faceted cyber technology cannot be handled by common standards and security policies.

Our Nation is treated like a hot spot for cyber attacks and information thefts by many countries. Due to this, we have taken a visionary initiative to curb and enervate the notoriously spreading cyber threats from various directions and dimensions.

A Common Platform to facilitate the experts to provide an effective solution for the complex and alarming problems in the society towards Cyber Security domain. We are developing innovative strategies and compliance procedures to curb the increasing complexity of the Global Cyber Threats.

The National Cyber Safety and Security Standards is an Autonomous Body which is controlled and monitored by the High Level Committee Chaired by Honourable Dr. Justice S. Mohan, Former Judge, Supreme Court of India and Chairman, National Cyber Safety and Security Standards.

Editorial Board

Table of Contents

Lesson 1

CYBER CRIME, TYPES OF CYBER CRIME AND TIPS ON PROTECTING YOURSELF AGAINST CYBER CRIME

Definition of Cyber Crime:

1. Crime committed using a computer and the internet to steal a person's identity or illegal imports or malicious programs. It's an unlawful act wherein the computer is either a tool or a target or both.

Weapons of Cyber Crime

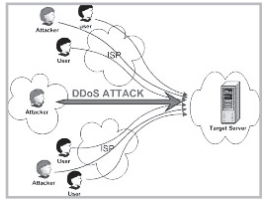
1. **Hacking:**

Unauthorized access to any computer or networks is known as 'HACKING'. That is accessing the information of others without proper authorization.

2. Data Diddling:

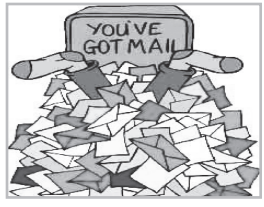
This is altering raw data just before a computer processes it and then changing it back after the processing is completed.

3. Denial of Service attack:



The Computer is flooded with more requests than it can handle which cause it to crash. Distributed Denial of Service (DDOS) attack is a example.

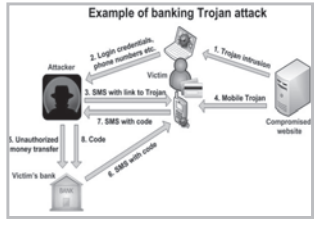
4. Email Bombing:



It refers to sending large numbers of mail to the victim, which may be an individual or a company by ultimately resulting into crashing.

5. Trojan attacks:

This term has its origin in the world 'Trojan horse'. In software field this means an unauthorized program, which passively gains control over another's computer by representing itself as an authorized program. The most common form of installing a Trojan is through e-mail.

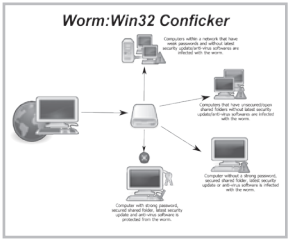


6. Web Jacking:

This term is derived from the term hijacking. In these kinds of offences the hacker gains access and control over the website of another. He may even manipulate or change the information of the website. This may be done for fulfilling political objectives or for money.

7. Virus/Worm Attacks:

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. Worms unlike viruses do not need the host to attach themselves to. They merely make functional copies of themselves and do this repeatedly till they eat up all the available space on the computer's memory.



8. Salami attacks:

This kind of Crime is normally prevalent in the financial institutions or for the purpose of committing financial crimes. An important feature of this type of offence is that the alteration is so small that it would normally go unnoticed.

9. Phishing:

Phishing refers to the receipt of unsolicited emails by customers of Financial Institutions, requesting them to enter their Username, Password or other personal information to access their Account for some reason. The fraudster then has access to the customer's online bank account and to the funds contained in that account.

10. Spamming:

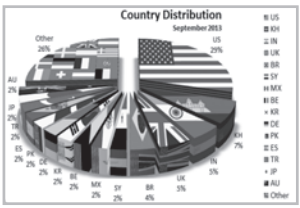
Electronic spamming is the use of electronic messaging systems to send unsolicited messages (spam), especially advertising, indiscriminately. The most widely recognized form of spam is e-mail spam.

11. Cyber Stalking:

Cyber Stalking is the use of the internet or other electronic means to stalk someone. Stalking generally involves harassing or threatening behavior that an individual engages in repeatedly.

Cyber Crimes in India

- The majority of Cybercrimes are centered on forgery, fraud and Phishing.
- India is the third-most targeted country for Phishing attacks after the US and the UK.
- Social networks as well as ecommerce sites are major targets.
- 6.9 million bot-infected systems in 2013.
- 14,348 websites defacements in 2013.
- 15,000 sites hacked in 2013.
- India is number 1 country in the world for generating spams.
- 29.9 million People fell victim to Cyber Crime.
- 17% of adults online have experienced Cybercrime on their mobile phone.



India's No 2 victim of cyber crime

Report says impact of attacks is immense, with many feeling cheated

Divyesh Singh

With increasing use of computers and the Internet through broadband penetration, the risk of being a victim of cyber crime has increased. Indian net users have been one of the most favourite targets of cyber criminals. In fact, a recent research report by global e-security solutions provider Norton has shown that 56% Indian web users have been victims of cyber crime.

The report pointed out that India is the second most victimised nation after China in terms of cyber attacks or cyber crime. It includes virus attacks, botnet attacks, online credit card frauds, lottery frauds, identity thefts, hacking attacks and attacks agencies cannot go beyond borders to take action against those who easily swindle money out of people's accounts.

The next time you surf the net, consider this: You may be a click away from becoming the next cyber crime victim.

The study by Norton revealed the staggering prevalence of cyber crime. Two-thirds (65%) Internet users globally, and over three-quarters (76%) Indian web surfers have fallen victim to cyber crimes, including computer viruses, online credit card fraud and identity theft.

Despite being left with a feeling of helplessness, only 39% Indian adults think that they will change their behaviour and take action legally when targeted.

The report revealed that the impact of such attacks has been immense on victims who feel ripped off or cheated. High emotional impact has affected their personal and professional lives.

Around 58% victims feel angry, while 51% have been left feeling annoyed and cheated and 46% among them are upset. Eighty-eight percent

Source from Internet

Safety Tips to Avoid Cyber Crime:

1. Use antivirus software and firewalls –keep them up to date.

2. Keep your operating systems up to date with critical security updates and patches.

3. Don't open emails or attachments from unknown sources.

4. Read Privacy policy carefully when you submit the data through internet.

5. Disable Remote Connectivity after completion of work.

6. Use hard-to-guess passwords. Don't use words found in a dictionary? Remember that password cracking tools exist.

   Examples: Simple (Weak) Passwords: abc12345,

12345678, india9876 / *Strong Passwords:* India@532#, Science$123#@

7. Back-up your computer data on disks or CDs often.
8. Never tell anyone either your PIN or password or write it down.

9. Never give anyone your card and tell them your PIN.
10. Keep your information up to date, if you change your address, inform your bank immediately.

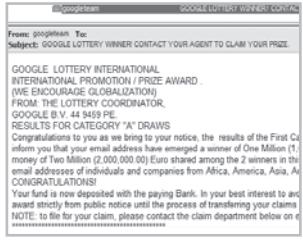
11. Check your statements carefully, go through your credit card and bank statements every month. Unexpected entries can be the first indication that somebody is stealing your money.
12. Learning to check your credit report is an effective tool in the fight against identity fraud. It gives you a snapshot of your borrowings and repayment history. You can easily spot unfamiliar accounts and suspicious balances.

13. Limit your social networking. It is dangerous to include basic information such as your full name and date of birth, pets or children's names and nicknames in your profile. Do not do it. These are the kind of details that you probably use for your passwords, never included such in your profile.

14. Do not carry your passport, driving license or Credit cards around unless you know you will need them, and never write down your PINs and your passwords. If your bag or wallet is stolen, you could be handing the thieves your identity.

15. Report thefts always to the police, your bank, and credit card issuers.

16. Never reply to emails and cold callers asking for details such as PINs, passwords and account numbers, and do not fill in your details on any unfamiliar email or website.



17. Put your card away safely before you leave the cash machine.

18. If you ask for a receipt, take it with you to check it against your statement when it arrives and then dispose of it safely.

Lesson 2

COMPUTER VIRUSES AND SOLUTIONS TO COMPUTER VIRUSES.

Computer Viruses

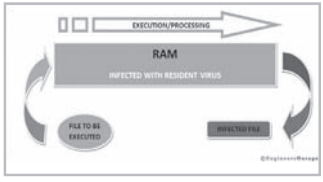
1. Computer virus is a kind of malicious software written intentionally to enter a computer without the user's permission or knowledge.

2. It has the ability to replicate itself, thus continuing to spread. Some viruses do little, but replicated viruses can cause severe harm or adversely affect program and performance of the system. A virus should never be assumed harmless and left on a system.

3. There are different types of computer viruses that can damage your system. Most common types of viruses are mentioned below:

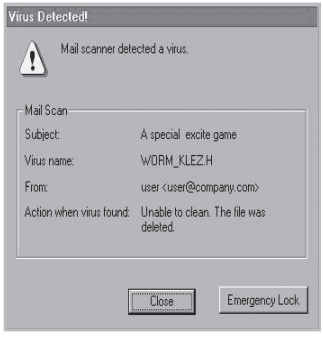
Types of Viruses

1. Resident Viruses:



These types of viruses are permanent and dwell in the RAM memory. From there they can overcome and interrupt all of the operations executed by the system: Corrupting files and programs that opened, closed, copied, renamed. Examples include: Randex, CMJ, Meve and MrKlunky.

2. Direct Action Viruses:

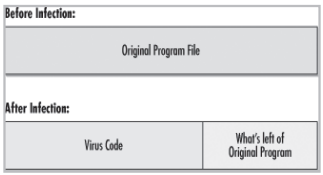


The main Purpose of these viruses is to replicate and take action when it is executed. When a specific condition is met, the virus will go into action and infect files in the directory or folder that it is, in the directories

that are specified in the AUTOEXEX.BAT file PATH. This batch file is always located in the root directory of the hard disk and carries out certain operations when the computer is booted.

3. Overwrite Viruses:

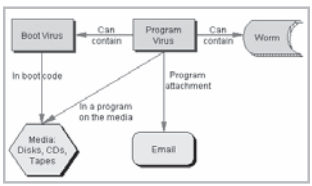
Viruses of this kind are characterized by the fact that they delete the information contained in the files that they infect, rendering them partially or totally useless once they have been infected. The only way to clean a file infected by an overwrite virus is to delete the file infected by an overwrite virus is to delete the file completely, thus losing the original content.



Examples of Overwrite viruses include: Way, TrjReboot, Trival. 88. D.

4. Boot Viruses:

These viruses affect the boot sector of a floppy or hard disk. This is a crucial part of a disk, in which information on the disk itself is stored together with a program that makes it possible to boot (start) the computer from the disk.



The best way of avoiding boot viruses is to ensure that floppy disks are write protected and never start your computer with an unknown floppy disk in the disk drive.

Examples of boot viruses include: Poly boot B, Anti EXE.

5. Macro Viruses:

Macro viruses infect files that are created using certain applications or programs that contain macros. These mini-programs make it possible to automate series of operations so that they are performed as a single action, thereby saving the user from having to carry them out one by one.

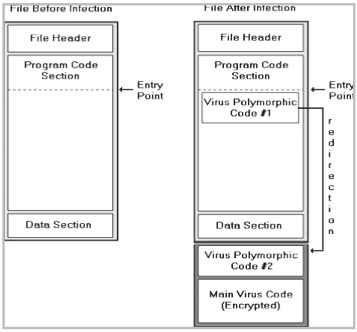
Examples of macro viruses include: Relax, MelissaA, Bablas, 097M/Y2K.

6. Directory Viruses:

Directory viruses change the paths that indicate the location of a file. By executing a program (file with the extension .EXE or .Com) which has been infected by a virus, you are unknowingly running the virus program, while the original file and program have been previously moved by the virus. Once infected, it becomes impossible to locate the original files.

7. Polymorphic Viruses:

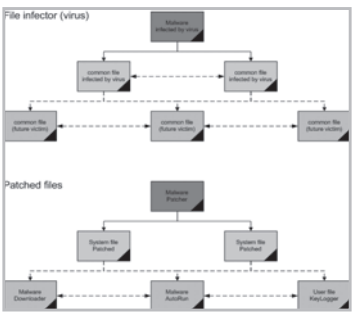
Polymorphic viruses encrypt or encode themselves in a different way using different algorithms and encryption keys every time they infect a system. This makes it impossible for anti-viruses to find them using string or signature searches (because they are different in each encryption) and also enables them to create a large number of copies of themselves.



Examples include: Elkem, Marburg, Satan Bug and Tuareg.

8. File Infectors:

This type of virus infects programs or executable files (files with an .EXE or .Com extension). When one of these programs is run, directly or indirectly, the virus is activated, producing the damaging effects it is programmed to carry out. The majority of existing viruses belong to this category, and can be



classified depending on the actions that they carry out.

9. Companion Viruses:

Companion viruses can be considered file infector viruses like resident or direct action types. They are known as companion viruses because once they get into the system they accompany the other files that already exist.

In other words, to carry out their infection routines, companion viruses can wait in memory until a program is run (resident viruses) or act immediately by making copies of themselves (direct action viruses).

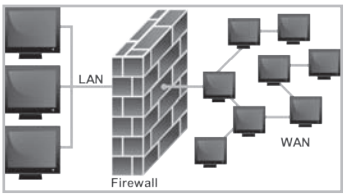
Examples include: Stator, Asimor, 1539, and Terrax 1069.

10. FAT Viruses:

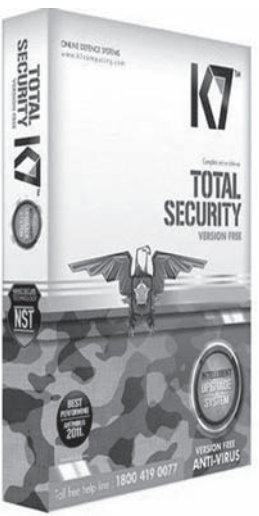
This file allocation table or FAT is the part of a disk used to connect information and is a vital part of the normal functioning of the computer. This type of virus attack can be especially dangerous, as it prevents access to certain sections of the disk where important files are stored. Damage caused can result in information losses from individual files or even entire directories.

Solutions to Computer Viruses

1. It is necessary to ensure that a desktop firewall is in place. A firewall is software or hardware that acts as a filter between your computer or network and the internet. Using a firewall prevents unauthorized access to your computer and is designed to stop worms.



2. Antivirus software will check your computer for viruses and alerts you of any virus, It is important to keep this software up to date, as new viruses are being created all the time.

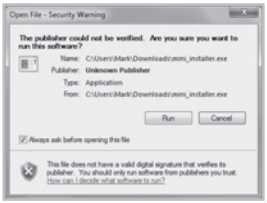


3. It is highly advisable to avoid disclosing personal information as much as possible. It is also a protective measure to open email attachments only from people you know. Be carefull about sharing files and downloading software, as these can easily spread viruses and hide spyware. (Sharing Files image) (Pen drive) (CD/DVD) Like this.

4. Be sure do a full back up of your system on a regular basis. The best way to clean up an infected file is to replace it with an original non-infected file. Not to mention the grief a current back up will save if a virus takes your system completely down. It's also a good idea to keep more than one set of backup in case the current one is infected before the virus is detected.

5. Don't allow your web browser to automatically run programs, such as MS Word or other programs through its e-mail program. Configure your browser to launch

WordPad or Notepad instead. One of the biggest and growing threats is the macro virus, which is spread through data processing and spread sheet programs.



6. Configure your web browsers to disable ActiveX, Java, and JavaScript. You'll lose some of the fun the Web's been known for, but you'll save your computer from contracting a virus and speed up your connection.

7. Know that the only way a virus spreads is either by launching an infected file or by booting an infected disk. You cannot get a virus by simply being online or by reading e-mail. You have to download and launch an infected file before it will spread. Therefore, do not launch any unsolicited executable files sent via e-mail.

Lesson 3

ONLINE FRAUD AND FINANCIAL TRANSACTION AND INSTRUCTIONS TO AVOID ONLINE FINANCIAL FRAUDS

Definition of Online Fraud:

"Online or internet fraud can be defined as any type of intentional deception that uses the internet. It includes fraud that occurs in chat rooms, message boards, web sites and through e-mail. It occurs in the form of deceitful solicitations and fraudulent transactions. Counterfeit fraud (skimming), lost or stolen cards, identity fraud, Cash-point Fraud, Facebook impersonation, Postal interceptions, and many more.

Types of Online Frauds:

1. Skimming:

Skimming is when someone copies the data from your card's magnetic strip onto another card without your knowledge. It can happen anywhere cash machines, shops, bars, restaurants and petrol stations. Always make sure you can see your card when you are making a transaction.

2. Lost or Stolen Cards:

It is easy to lose your card or have it stolen. You could drop it in a shop when you take something else out of your pocket, or you could put it down and forget to pick it up.

3. Identity Fraud:

If personal details like your address, passport number and national insurance number or social security number are stolen they can be used to set up online accounts or to apply for credit cards; and apply for benefits in your name without you knowing. Criminals may try to get your credit card details by sending emails that appear to be from a reputable online organization like a bank or a credit company. They may encourage you to enter your credit card details or password on a fake website.

4. Credit Card Fraud:

"Credit card and debit card fraud is costing the industry more than $452 million a year. The reason was mainly due to counterfeiting cards, which more than doubled during 2000, as well as a 94% rise in fraud using stolen credit card details to pay for things over the telephone or internet.

5. Social Media Impersonation:

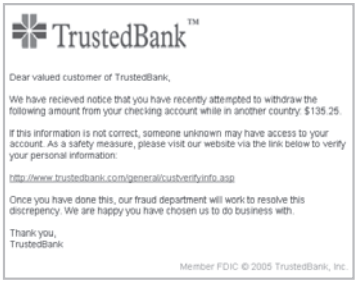
The crime one should most worry about is Social Media impersonation. A criminal who hacks into your Facebook account can learn and steal a great amount of information about you. He or She can gain trusted access to friends and family. There have been many stories that show Facebook friends can easily be tricked into sending money.

6. Postal Interceptions:

If you are expecting a new card or cheque book through the post and it does not arrive, call your bank immediately or report to your local post office.

7. Email Fraud:

Fraudulent email activity is increasing. These emails may appear to be from legitimate companies that you do business with such as your bank, an online auction site, or your internet service provider. You are often asked to validate or confirm your personal information or opening an attachment. These messages can contain viruses, known as 'Trojan


TrustedBank™

Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.

horse' programs, designated to record your keystrokes. These emails can also direct you to counterfeit web sites that appear to be genuine.

Avoiding Online Financial Fraud

1. Buying and selling online is just as safe as ordering goods over the phone, but you should be aware that dishonest people may try to convince you to give them your card or personal details. (Don't Provide Personal Details in Online Transactions, Prefer Cash on Delivery of Goods, because it is the way to avoid the providing personal Details like Debit Card Number and Pin Number)

2. Before you buy anything online make a note of the address of the company that you are buying from. This should include details of the telephone and/or fax number. Never rely on just an email address.
   It is of utmost necessity that you use secure sites always. These sites have 'https' in front of the web address which indicates that the company has been independently checked to make sure they are who they say they are. A yellow padlock symbol will appear in

the browser window to show the payment process is secure when buying online.

The following types of URL's are may not be Secure:
Ex 1: http://www.irctc.co.in
Ex 2: http://www.onlinesbi.com
The Following types of URL's are more secured:
Ex 1: https://www.irctc.co.in
Ex 2: https://www.onlinesbi.com

3. Other things to bear in mind should include the following:
   A. Check the returns policy of the Product when you buy it from Online.
   B. Print out a copy of your order and any acknowledgement you receive.
   C. Check your bank statement carefully against anything you receive.

RETURN POLICY

Mandate loves you, and we want to make you happy. Unfortunately, due to the one-of-a-kind and/or small run nature of our garments, returns are difficult for us to accept.

When making an order, please pay careful attention to item details and sizing information. If you have any questions, we're happy to help; send all product inquiries to mandateofheaven1982@hotmail.com and we'll get back to you as soon as possible.

Silhouette plays a huge role in our designs; a Mandate piece isn't complete until it's filled out by a lovely human body. However, lovely bodies come in an astounding array of shapes and proportions. Standard off the rack sizes don't fit most people as well as they should; it would be impossible to make them do so. Thus, we encourage our customers to have their items personally tailored whenever possible. Please keep this possibility in mind when making your Mandate selections. Remember, things can usually be taken in, but they can't always be let out.

If your Mandate purchase does not fit and cannot be altered, we may be able to offer you an exchange. In this event, please contact us as soon as you receive your item; exchange requests received more than 24 hours after the receipt of package will not be considered.

Thank you for your interest and understanding.

XX Mandate

Taxpayers Counterfoil

SPACE FOR BANK SEAL

ICICI Bank

(Checking Messages or receipts from bank whenever we receive)

D. Don't write your passwords and Pin Numbers either in Note Books and Slips.

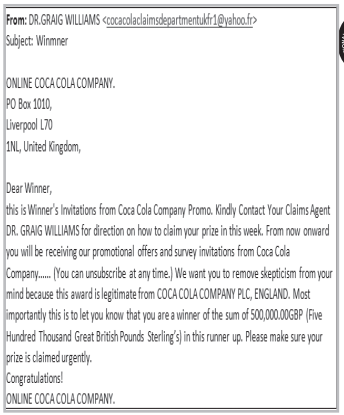
E. Strong passwords have eight characters or more, and use a combination of letters, numbers, and symbols. (Strong and don't write anywhere)

Weak	Medium	Strong
All numbers or all letters	Alphanumeric	Alphanumeric with a mix of upper and lower case letters
beckeriscool	becker2cool	B3cker2C00l

F. Familiarize yourself with a Web site's privacy policy, especially if you are asked to provide confidential and/or personal data.

4. You will protect yourself by keeping in mind that the internet provides criminals with an easy way to

contact thousands of people at a time. Examples include emails offering the chance to take part in money making scheme, or claiming you are the winner of a prize draw.



From: DR.GRAIG WILLIAMS <cocacolaclaimsdepartmentukfr1@yahoo.fr>
Subject: Winmner

ONLINE COCA COLA COMPANY.
PO Box 1010,
Liverpool L70
1NL, United Kingdom,

Dear Winner,
this is Winner's Invitations from Coca Cola Company Promo. Kindly Contact Your Claims Agent DR. GRAIG WILLIAMS for direction on how to claim your prize in this week. From now onward you will be receiving our promotional offers and survey invitations from Coca Cola Company..... (You can unsubscribe at any time.) We want you to remove skepticism from your mind because this award is legitimate from COCA COLA COMPANY PLC, ENGLAND. Most importantly this is to let you know that you are a winner of the sum of 500,000.00GBP (Five Hundred Thousand Great British Pounds Sterling's) in this runner up. Please make sure your prize is claimed urgently.
Congratulations!
ONLINE COCA COLA COMPANY.

5. You can avoid being a victim of internet fraud by doing the following:
   * Remember if something sounds too good to be true, it is usually better to seek independent financial advice before making investments.
   * Only do business with companies that you recognize or know through recommendation or by someone you trust.
   * Do not judge a company on how professional its website may look. If in any doubt, you can check if a company is genuine by looking at its profile on Companies House or Financial Services Authority (FSA) websites or other associated public services

Lesson 4

CYBER WAR AND CYBER TERRORISM AND WAYS ON HOW TO PREVENT CYBER TERRORISM FROM HAPPENING

Cyber Terrorism:

1. The use of computing resources to intimidate, coerce or harm people, places or systems we depend upon.

Characteristics of Cyber Terrorism:

1. They act must have scale and publicity.
2. Cyber Terrorism is safe and profitable.
3. Cyber Terrorism is difficult to counter without the rights expertise and understanding of the Cyber terrorist's mind.
4. Relatively anonymous.
5. Unlike other acts of terrorism, if the Cyber terrorist loses today, he/she does not die - he/she learns what did not work, and will use that information against you tomorrow.

Cyber Warriors:

1. The Cyber Terrorist will make certain that the population of a nation will not be able to eat, to drink, to move, or to live.
2. The people Charged with the protection of their nation will not have warming, and will not be able to shut down the terrorist, since that Cyber Terrorist is relatively hard to locate and could be on the other side of the world or sitting at a personal computer in your public library.

Psychology of Modern Warfare and Hacking:

- For Fun (31.4%)
- Want to be best defacer (17.2%)
- No reason Specified (14.7%)
- Political Reasons (11.8%)
- Patriotism (10.9%)
- As a Challenge (10.8%)
- Revenge (3.3%)

Forms of Cyber Terrorism

- Privacy Violation
- Secret information appropriation and data theft
- Demolition of e-governance base
- Distributed denial of services attack

Critical Infrastructure affected by Cyber Terrorism:

1. Government Operations
2. Emergency Services
3. Telecommunications
4. Electrical Energy
5. Gas & Oil Storage and Delivery

6. Water Supply Systems
7. Banking & Finance
8. Transportation

Factors Contributing to the Existence of Cyber Terrorism:

1. Dependence on Network Infrastructure and the Internet.
2. Lack of Understanding of Security Risks.
3. Lack of Funding for Adequate Network Security Tools.
4. Perception that the steps to combat cyber terrorism will make life inconvenient.
5. The ease and of doing the act.
6. Difficulty in tracking the Cyber Terrorist.

Direct Cost Implications:

1. Loss of sales during the disruption.
2. Staff time, network delays, intermittent access for business users.
3. Increased insurance costs due to litigation.
4. Loss of intellectual property-research, pricing, etc.
5. Costs of forensics for recovery and litigation.
6. Loss of critical communications in time of emergency.

Indirect Cost Implications:

1. Loss of Confidence and credibility in our financial systems.
2. Tarnished relationships & public image globally.
3. Strained business partner relationships-domestic and internationally.
4. Loss of future customer revenues for an individual or group of companies.
5. Loss of trust in the Government and Computer industry.

Who are the Cyber Terrorists?

1. Crackers: The transition may be motivated by money or prestige. Usually, this transition will occur without the cracker's cognizance.
2. Young, Educated people brought into the folds of terrorist groups- This new generation will have the talent to execute the acts of Cyber terrorism.

Main Weapons:

1. Building / Office Security
2. Desktop / Laptop Computer Security
3. Network Security
4. Disaster Recovery planning

Tips to Prevent from Cyber Terrorism:

1. Cooperate and share intelligence among all agencies.
2. Learn the new rules, the new technologies, and the new players.
3. The tools of a counter-Cyber Terrorist team must be real time and dynamic, as the weapons will continually change.
4. Make building, network and desktop security a priority.
5. Report instances of Cyber Crime to local law enforcement agencies.
6. Recognize the most vital information and always keep it in the safest possible Place.
7. Develop a strong password.
8. Disable any application that seems unnecessary.
9. If you are ever unsure about the safety of a site, or receive suspicious email from an unknown address, don't access it. It could be trouble.

Honorable Dr. Justice S. Mohan, Former Judge, Supreme Court of India and Chairman, National Cyber Safety and Security Standards, Honourable Dr. Justice P. Jyothimani, Former Judge, Madras High Court, Shri. Dr. G.A. Raj Kumar, I. A. S, Chairman, National Executive Committee, National Cyber Safety and Security Standards, Shri. S. Machendranathan, I. A. S, Former Cabinet Secretary (Coordination And Public Grievances) and other dignitaries at National Cyber Safety and Security Standards Summit- 2013, Chennai, Tamil Nadu.

Releasing of National Cyber Crime Reference Handbook at Raj Bhavan, Chennai by His Excellency Dr. K. Rosaiah, Governor of Tamil Nadu, Honorable Dr. Justice S. Mohan, Former Judge, Supreme Court of India and Chairman, National Cyber Safety and Security Standards, Shri. Dr. G.A. Raj Kumar, I. A. S, Chairman, National Executive Committee, National Cyber Safety and Security Standards, Dr. S. Amar Prasad Reddy, Additional Director - General, National Cyber Safety and Security Standards and other dignitaries.

PRESS RELEASES - NATIONAL CYBER CRIME REFERENCE HANDBOOK

Coming, cyber security guidelines

OUR BUREAU
Chennai, May 7

The National Cyber Safety and Security Standards will release a comprehensive set of guidelines for private and public sector companies to secure their online data.

Slated for unveiling by the end of this calendar year, the guidelines will help banks, government enterprises and private firms privy to sensitive material guard their data on the Internet, S Mohan, Chairman, National Cyber Safety and Security Standards, told *Business Line* at an event here today.

"We are putting together an exhaustive list, because there is a diverse set of private enterprises in the country. We are not mandating any rules. They are just guidelines," he said.

The move to release guidelines comes at a time when security attacks on India are growing more frequent. In a handbook it released today, the security agency describes a March 2010 attack that stole revelatory information from Indian Defence Ministry – "The India-focussed spy ring used social networking service providers such as twitter, Google and others to take over control of computers in India."

The report says Chinese threats to India through a parasite program called BOTNET are rampant; an instance in March 2010 of security breach into Prime Minister's Office was traced back to this malware.

Collaboration between States and the Centre in exchanging information of attacks and installing safety measures will minimise such attacks, says Amar Prasad Reddy, Additional Director-General, National Cyber Safety and Security Standards. He said the organisation is now trying to include Internet Service Providers in their operations, so that websites publishing confidential material can be immediately taken down.

The Hindu Business Line, Pg No.07, 08 May 2014, Chennai

Handbook on cyber attacks, information thefts released

Chennai: Tamil Nadu governor K Rosaiah on Wednesday released 'National Cyber Crime National Handbook. Published by the National Cyber Safety and Security Standards, it is aimed at informing people about cyber-attacks and information thefts.

It includes chapters like cyber hacking, e-commerce, e-mail security, cyber fraud and cyber attacks, cloud computing, evidentiary value of video conferencing, privacy and electronic surveillance and data security and privacy.

National Cyber Safety and Security Standards chairman S Mohan said the guidelines would help secure information, communications and systems of various organizations. "The autonomous body is doing extensive research and take new initiative to protect the country from cyber threats," he said.

The book provides a common platform for experts to analyse issues involved in cyber security, he said adding the country was a "hot-spot" for such attacks. "Today, electronic devices are no longer confined to computers but are pervasive in everyday life. They range from smart phones to GPS devices and from health monitoring devices to defibrillators," he said.

The book is being distributed free to all state and central government departments. TNN

The Times of India, Pg No.05, 08 May 2014, Chennai

साइबर क्राइम पर हैंडबुक का विमोचन

चेन्नई

chennai@patrika.com

राज्यपाल डा. के. रोसैया ने बुधवार को राजभवन में नेशनल साइबर क्राइम रेफरेंस हैंडबुक का विमोचन किया। यह पुस्तक राज्य व केंद्र सरकार के विभागों को निशुल्क दिया जाएगा। नेशनल साइबर सेफ्टी एंड सिक्योरिटी स्टैंडर्ड्स की ओर से यह पहल की गई है। इस पुस्तक में कई चैप्टर हैं। यह पुस्तक उन सभी लोगों के लिए उपयोगी है जो सरकारी और निजी क्षेत्र, कारपोरेट कंपनी या शैक्षणिक संस्थानों में काम करते हैं। इससे उनका महत्वपूर्ण इन्फ्रास्ट्रक्चर सुरक्षित रहेगा।

कि साइबर अपराध बढ़े हैं ऐसे में साइबर खतरों तथा अपराधों की रोकथाम व नियंत्रण समय की जरूरत है। साइबर सेफ्टी और सिक्योरिटी का

साइबर सेफ्टी एंड सिक्योरिटी स्टैंडर्ड्स के चेयरमैन डा.एस.मोहन ने कहा कि बड़ी मात्रा में सूचना, अनुभव और कौशल का ज्ञान जरूरी

Rajasthan Patrika,Page No.02, 08 May 2014, Chennai

ఇది సైబర్ యుగం

'నేషనల్ సైబర్ క్రైమ్ రెఫరెన్స్ హ్యాండ్ బుక్' ఆవిష్కరణలో గవర్నర్ రోశయ్య

ఆంధ్రజ్యోతి, చెన్నై: ఇటీవల కాలంలో ఐటీ విప్లవం పలు అవకాశాలను సృష్టిస్తోందని గవర్నర్ డాక్టర్ కె. రోశయ్య అన్నారు. ఆయన బుధవారం రాజ్‌భవన్, దర్బార్ హాల్లో జరిగిన కార్యక్రమంలో ముఖ్యఅతిథిగా పాల్గొని 'నేషనల్ సైబర్ క్రైమ్ రెఫరెన్స్ హ్యాండ్ బుక్' విడుదల చేశారు. అనంతరం ఆయన మాట్లాడుతూ, ఇవ్వాళ సమాచార విప్లవం ప్రతి ఇంటికీ చేరిందన్నారు. దీనితో ఈ-కామర్స్, ఈ-గవర్నెన్స్, ఈ-ట్రేడ్, ఈ-బ్యాంకింగ్, ఈ-కమ్యూనికేషన్స్, ఈ-సెక్యూరిటీ వంటివి ప్రాధాన్యత సంతరించుకున్నట్టు తెలిపారు. ఇక ఇంటర్నెట్ వాడకం తో సమాచార వ్యవస్థలో భారీ మార్పులు చోటు చేసుకున్నట్లు తెలిపారు. అయితే, ఈ సమయంలోనే భారత సైబర్ వనరులపై ముష్కరుల దాడులు కూడా పెరిగినట్లు గవర్నర్ తెలిపారు. భారత రక్షణశాఖ వెబ్ సైట్లను సైతం హ్యాక్ చేయడానికి ప్రయత్నాలు జరుగుతున్నాయన్నారు. 2005-2010 మధ్య సైబర్ వినియోగం రెండింతలయినట్టు గణాంకాలు చెబుతున్నాయన్నారు. అయితే ఆస్థాయిలో సైబర్ నిపుణులు లేకపోవడం విచారకరమన్నారు. మన దేశంలో కేవలం 556 మంది సైబర్ నిపుణులున్నారని, ఇదే అమెరికాలో 91 వేలు, చైనాలో 1.2 లక్షలు రష్యాలో 7 వేలకు పైగా నిపుణులు అందుబాటులో వున్నట్టు తెలిపారు. ప్రస్తుతం సైబర్ నేరాలు పెద్ద సవాలుగా పరిణమించాయన్నారు. ఈ సైబర్ నేరాలను నియంత్రించడానికి జాతీయ సైబర్ రక్షణ వ్యవస్థ ఏర్పాటుయిందన్నారు. దేశవ్యాప్తంగా అన్ని వర్గాల వారికీ సైబర్ నేరాలపై వీరు అవగాహన కలిగించే ప్రయత్నం చేస్తున్నట్టు తెలిపారు. ఇందులో భాగంగానే ఈ పుస్తకాన్ని ప్రచురించినట్లు తెలిపారు. అనంతరం జాతీయ సైబర్ సొసైటీ అధ్యక్షుడు, సుప్రీం కోర్టు మాజీ న్యాయమూర్తి డాక్టర్ ఎస్. మోహన్‌ను గవర్నర్ సత్కరించారు. ఈ కార్యక్రమంలో ఇంకా రిటైర్డ్ ఐఏఎస్ అధికారి జీపీ రాజ్‌కుమార్ తదితరులు కూడా పాల్గొన్నారు.

పుస్తకావిష్కరణలో గవర్నర్ రోశయ్య, రిటైర్డ్ ఐఏఎస్ అధికారి రాజ్‌కుమార్, మాజీ న్యాయమూర్తి మోహన్ తదితరులు

Andhra Jyothi, Page No.10, 08 May 2014, Chennai

పెరుగుతున్న సైబర్ నేరాలు

అన్నానగర్, న్యూస్‌లైన్:

మంది కోసం తలపెట్టిన ఇన్ఫర్మేషన్ టెక్నాలజీ రంగాన్ని దుర్వినియోగం చేస్తూ కొందరు సైబర్ నేరాలకు పాల్పడుతున్నారని రాష్ట్ర గవర్నర్ కె.రోశయ్య ఆవేదన వ్యక్తం చేశారు. ఇంటర్‌నెట్, ఎలక్ట్రానిక్ పరికరాలను సంఘ వ్యతిరేక శక్తులుగా వాడడం పట్ల ఆయన తీవ్ర విముఖతను వ్యక్తం చేశారు. బుధవారం రాజ్‌భవన్ దర్బార్ హాలులో నేషనల్ సైబర్ సొసైటీ సేఫ్టీ అండ్ సెక్యూరిటీ స్టాండర్డ్స్ ఏర్పాటు చేసిన గ్రంథావిష్కరణ సభలో ఆయన నేషనల్ సైబర్ క్రైం రిఫరెన్స్ హ్యాండ్ బుక్ అనే సాంకేతిక పుస్తకాన్ని ఆవిష్కరించి ప్రసంగించారు. సైబర్ నేరాలను అరికట్టడంలో సెక్యూరిటీ స్టాండర్డ్స్ అవిశ్రాంతంగా కృషి చేయడం పట్ల ఆయన సంతృప్తిని వ్యక్తం చేశారు. ఆయన ముఖ్య అతిథిగా విచ్చేసిన భారత సుప్రీంకోర్టు మాజీ జడ్జి ప్రస్తుత సెక్యూరిటీ స్టాండర్డ్స్ విభాగం చైర్మన్ డాక్టర్ ఎస్ మోహన్‌ను ఘనంగా సత్కరించారు. డాక్టర్ ఎస్ మోహన్ మాట్లాడుతూ, ఇంటర్నెట్‌లో సెక్యూరిటీ అనేది ప్రతివారు తెలుసుకోవాల్సిన అంశం అన్నారు. సమాచారం తెలుసుకోవడానికి నిర్దేశించిన అంతర్జాలాన్ని నేరాల కోసం ఉపయోగించే వారి సంఖ్య నానాటికీ పెరుగుతున్న దృష్ట్యా, వినియోగదారులను చైతన్యవంతుల్ని చేసేందుకు ఈ పుస్తకాన్ని వెలువరించామన్నారు. ఈ పుస్తకం ఎథికల్ హ్యాకింగ్, నెట్‌లోని వినియోగదారుల వ్యక్తిగత సమాచారాన్ని ఎలా సంరక్షించుకోవాలో విశదీకరిస్తుందన్నారు. ఈ కార్యక్రమంలో మాజీ కలెక్టర్ డాక్టర్ జీపీ రాజ్‌కుమార్, మాజీ ఆఫీస్ చీఫ్ సెక్రటరీ డాక్టర్ ఎస్ అమర ప్రసాదరెడ్డి, సెక్యూరిటీ స్టాండర్డ్స్ అడిషనల్ డైరెక్టర్ ఈజె రాజ్ తదితరులు పాల్గొన్నారు.

గ్రంథావిష్కరణ సభలో పాల్గొన్న గవర్నర్ రోశయ్య, మోహన్, రాజ్‌కుమార్, అమర ప్రసాదరెడ్డి, ఈజే రాజ్

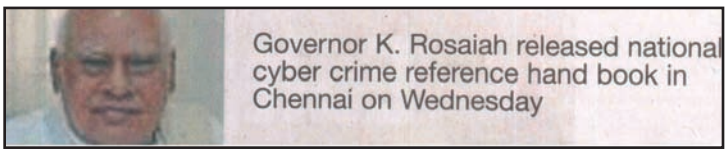
Sakshi, Page No.04, 08 May 2014, Chennai

సైబర్ నేరాలతో తీవ్ర ముప్పు

చెన్నై, మ్యూహంటుడే: ఆధునిక పరిజ్ఞానంతో ప్రైవేటు, ఆరోగ్య సంరక్షణ, బయోటెక్నాలజీ, ఆటోమొబైల్, మందుల పరిశ్రమలు వంటి ఆన్ని రంగాల్లో దేశం ముందంజలో ఉమనస్తుందని గవర్నర్ కొణిజేటి రోశయ్య పేర్కొన్నారు. రాజ్‌భవన్‌లోని దర్బార్ హాలులో జరిగిన నేషనల్ సైబర్ సేఫ్టీ అండ్ సెక్యూరిటీ స్టాండర్డ్స్ (ఎస్‌సీఎస్‌ఎస్) ఏర్పాటు చేసిన కార్యక్రమంలో ఆయన ప్రసంగించారు. బలే రంగం ప్రతి శంతో ఈ-బ్రేడ్, ఈ-గవర్నెన్స్, ఈ-కామర్స్, ఈ-కమ్యూనికేషన్, ఈ-బ్యాంకింగ్, ఈ-సెమ్యూటిక్, టెలిమెడిసిన్ వంటి ఎన్నో సౌకర్యాలు ప్రజలకు చేరువయ్యాయని పేర్కొన్నారు. నిత్య జీవనంలో భాగమైన ఈ రంగంలో జరుగుతున్న సైబర్ నేరాలతో అనేక సమస్యలు కూడా చవిచూడాల్సి వస్తోందన్నారు. ఈ విషయంలో అప్రమత్తమై నేరాలు నియంత్రణ దిశగా ఆన్ని సంస్థలు కృషి చేయాలని సూచించారు. ఈ సందర్భంగా ఎమ్‌ఎస్‌ఎమ్‌ఈ రూపొందించిన నేషనల్ సైబర్ క్రైం రిఫెరెన్స్ హ్యాండ్ బుక్‌ను గవర్నర్ ఆవిష్కరించారు. ఈ కార్యక్రమంలో ఎమ్‌ఎస్‌ఎమ్‌ఈలకు చెందిన ఉన్నత ప్రతినిధులు సుప్రీంకోర్టు మాజీ న్యాయమూర్తి జస్టిస్ ఎస్ మోహన్, డాక్టర్ రాజేశకుమార్, డాక్టర్ ఎస్ ఆమర్, ఈశే రాజా తదితరులు పాల్గొన్నారు.

పుస్తకావిష్కరణలో గవర్నరు రోశయ్య తదితరులు

Eenadu, Page No.03, 08 May 2014, Chennai



Governor K. Rosaiah released national cyber crime reference hand book in Chennai on Wednesday

Deccan Chronicle, Page No.07, 08 May 2014, Chennai

'Create awareness on cyber laws'

Express News Service

Chennai: Governor K Rosaiah on Wednesday warned that cyber crime was emerging as a serious threat globally, with about 42 million cyber crimes reported in India every year.

Releasing the National Cyber Crime Reference Hand Book, brought out by the National Cyber Safety and Security Standards and the Ministry of MSME, he said that the Internet had brought about a huge change in modes of communication and access to information. "Our nation has become a hotspot for cyber attacks and information theft, he pointed out. "Heightening security for our systems has become imperative, and co-ordinated, sustained and institutionalised efforts are needed to protect critical network infrastructure from hackers and cyber criminals."

Dignitaries at the release of National Cyber Crime Reference Hand Book

The Governor warned that cyber crime had emerged as a serious threat, with studies showing seven out of 10 adults becoming victims of different modes of cyber crime in their lifetime.

Lauding the initiatives launched by the National Cyber Safety and Security Standards to curb and enervate the spreading cyber threats, he said creation of awareness on cyber laws, sensitising the public on safety measures, identifying fake host pages and creation of alertness and a sense of vigil against hackers was imperative.

"Educating people on these lines is the need of the hour," he added.

The New Indian Express, Supplement. City Express
Page No.04, 08 May 2014, Chennai

Honourable Shri. Justice B. K. Patel, Judge, Orissa High Court & Member, Odisha Judicial Academy Committee, Honourable Dr. Justice P. Jyothimani, Former Judge, Madras High Court and Judicial Member, Eastern Bench, National Green Tribunal, New Delhi, Honourable Mr. Justice T.N. Vallinayagam, Former Judge, Madras High Court and other dignitaries, Guests & Speakers at National Cyber Safety and Security Standards Summit- 2014, Coimbatore, Tamil Nadu.

Delegates at National Cyber Safety and Security Standards Summit- 2014, Coimbatore, Tamil Nadu.

National Cyber Safety and Security Standards Summit – 2014 Press Releases

கருத்தரங்கை ஒடிசா ஐகோர்ட்டு நீதிபதி படேல் தொடங்கி வைத்து பேசியபோது எடுத்தபடம்.

இணையதள குற்றங்களை தடுப்பது பற்றிய தேசிய கருத்தரங்கு

கோவையில் தொடங்கியது

கோவை,செப்.20-

'இணையதள குற்றங்களை தடுப்பது பற்றிய தேசிய கருத்தரங்கு கோவையில் நேற்று தொடங்கியது.

தேசிய கருத்தரங்கு

தேசிய சைபர் பாதுகாப்பு மற்றும் பாதுகாவல் தர தேசிய கருத்தரங்கு கோவை பி.எஸ்.ஜி. கலை அறிவியல் கல்லூரியில் நேற்று தொடங்கியது. இதை ஒடிசா ஐகோர்ட்டு நீதிபதி படேல் தொடங்கி வைத்து பேசினார்.

இதில் மத்திய அரசு ஒருங்கிணைப்பு மற்றும் பொதுதுறை நிர் முன்னாள் செயலாளர் மச்சேந்திரநாதன் கலந்து கொண்டு பேசினார். அப்போது அவர் பேசியதாவது-

உலகின் ...

அடிப்படையாக கொண்டது.

விழிப்புணர்வு ஏற்படுத்த வேண்டும்

இது நமது சமுதாயத்துக்கு உலக அளவில் பெரிய அச்சுறுத்தலாக விளங்கி வருகிறது. இதுபற்றி மக்கள் இடையே விழிப்புணர்வை ஏற்படுத்த வேண்டியது அவசியமாகிறது. எனவே இணையதள மோசடிகளை கட்டுப்படுத்த உரிய நடவடிக்கைகளை எடுக்க வேண்டும்.

இவ்வாறு அவர் பேசினார்.

கருத்தரங்கில், மத்திய அரசின் முன்னாள் கூடுதல் முதன்மை செயலாளர் ஜி.ஏ.ராஜ்குமார், சிக்கிம் மாநில விளையாட்டு மற்றும்

Daily Thanthi Sep 20 Pg 11

Experts call for indigenous anti-virus to protect data

TIMES NEWS NETWORK

PSreedharan

National Cyber Safety and Security Standards Summit was held in city on Friday

Coimbatore: Cyber experts who met at a conference in Coimbatore on Friday said India should have its own anti-virus software to prevent the possibility of sensitive data being accessed by foreign companies who develop anti-virus.

The experts who met in Coimbatore under the aegis of National Cyber Safety and Security Standards Summit wanted the government to find ways to deal with foreign search engines like Google that are reluctant or delay initiation of action on complaints. Judges and bureaucrats too, who were part of the deliberations, underlined the need for urgent steps to prevent cyber crimes.

"I have been under cyber attack twice," said Orissa high court judge B K Patel. "The first experience was in 2004 when I found two transactions done from my account without my knowledge. The second time my social networking site account was hacked," Patel said. "There are so many questions on cyber safety, but no answers," he said. So many are turning to internet for various reasons like social networking and banking, but most people are not aware of threats in the cyber world.

Former cabinet secretary S Machendranathan said that updating safety standards should continue on a par with technology development. K Jayakumar, principal secretary of sports and youth affairs in Sikkim shared the same view noting that a mechanism to ensure order should be developed to preempt cyber crimes.

Amar Prasad Reddy from National Cyber Safety and Security Standards, a self governed organization, said that the objective of the summit was to bring together government, private and public enterprises and evolve a common standards for cyber safety.

Times of India Sep 20 Pg 5

'Response to Cyber Crime Complaints Slow'

Express News Service

Coimbatore: Google, Yahoo and Facebook took more than 48 hours to respond to cyber crime complaints as none of these search engines and social networking sites had their nodal officers appointed in India, say cyber crime experts who participated in the National Cyber Safety and Security Standards Summit '14 here on Friday.

The Additional Director-General, National Cyber Safety and Security Standards, Amar Prasad Reddy said it was difficult or almost impossible to sort out the details of criminals in most of the cyber crime cases as the cyber crime police had to contact centres of all the popular search engines and social media sites outside the country for help. "Even before the objectionable content is taken down, damage could already be done to the victim as lakhs of people are active on these sites and chances are that certain people have saved it to their personal devices," he added.

The National Cyber Coordination Centre (NCCC) to be set up at a cost of ₹700 crore by the Centre will act as the national cyber intelligence cell which will help communicate with all the social media sites and search engines, he added.

Cyber crime experts said that as far as Tamil Nadu was concerned, cyber criminals targeted women and children. Women were threatened by posting their morphed personal pictures and contact numbers on websites and social media sites.

Besides, contact and financial details of parents were collected from children through bogus websites. Most of the cyber crimes were perpetrated with a financial motive and the bank accounts were hacked. Most of the time, banks do not entertain complaints from victims as they had no proof to support their claim.

According to experts, the recent trend in India was to open bank accounts for those who were ignorant of banking system and later use their credit/debit cards to get loans. However, it was impossible for police to track down the criminals.

Around 18 State government representatives, eight High Court judges and police representatives from various states participated.

The New Indian Express Sep 20 Pg 3

Call to establish Fast Track Courts to try cases of cyber crime

'Convictions will result in better awareness of cyber laws'

Staff Reporter

COIMBATORE: Former judges of the Madras High Court Justice T.N. Vallinayagam and Justice P. Jyothimani suggested slapping Goondas Act against persons indulging in cyber crimes and setting up fast track courts exclusively hear cyber crimes cases for bringing down cyber crimes. They were here on Saturday for addressing delegates on the two-day National Cyber Safety and Security Standards Summit – 2014.

Mr. Jyothimani proposed establishing special fast track courts to hear cyber crime cases. He said that doing so would result in pouring in of more such cases and their convictions would result in better awareness among the people on cyber laws – and result in a drop in cyber crimes. The judge said that globally, India stands 3rd in internet usage with as many as 14 million websites visited by people of the country every year. He also expressed the need for allocation of funds to improve cyber security. He claimed that last year the Ministry of Communication and Information Technology sought Rs. 1,500 crore for this purpose. "But, the government sanctioned only Rs. 500 crore," he said.

He said that in India, The Information Security Act was passed in the 2000 and was amended in 2008 – with provisions for crimes such as 'cyber stocking, web defacing and pornography. Noting that there are cyber labs only in Mumbai, Bengaluru, Pune and Kolkata, he added that the labs too have only limited resources. The Government should improve the infrastructure of these labs and frame a cyber policy, he added. Mr. Vallinayagam felt that Goondas Act should be strengthened and slapped against cyber crime offenders.

"We are still using laws that were framed by the British. We should enforce and modify laws to suit our society. A Roman states that fear should be always in the mind of the criminal, else he will expand his horizon," he said. He also expressed the need for encouraging private organisations to improve cyber security as he felt that the police alone would not be able to handle cyber crime investigations.

The Hindu Sep 21 Pg 5

സൈബർ കേസുകൾ വിസ്തരിക്കാൻ പ്രത്യേക കോടതി വേണം -മുൻ ഹൈക്കോടതി ജഡ്ജി പി. ജ്യോതിമണി

കോയമ്പത്തൂർ: സൈബർ കുറ്റകൃത്യങ്ങളും വർധിച്ചുവരുന്ന സാഹചര്യത്തിൽ ഇത്തരം കേസുകളും വിചാരണ ചെയ്യാൻ പ്രത്യേക കോടതി ആവശ്യമാണെന്ന് മുൻ മദിരാശി ഹൈക്കോടതി ജഡ്ജി പി. ജ്യോതിമണി അഭിപ്രായപ്പെട്ടു.

ദേശീയ സൈബർ സേഫ്റ്റി അഡ്വൈസറായ ജസ്റ്റിസ് ജ്യോതിമണി സൈബർസുരക്ഷാ ഉന്നതസമിതിയുടെ രണ്ടുദിവസത്തെ സമ്മേളനത്തിൽ പ്രസംഗിക്കുകയായിരുന്നു. പ്രത്യേക കോടതികളുംതന്നെ പോരാ കേസുകളും അന്വേഷിക്കാനുള്ള പോലീസുകാരെ പരിശീലിപ്പിക്കണം. പ്രഥമവിവരറിപ്പോർട്ടാണ് കേസിന്റെ തുടക്കം. പ്രഥമവിവരറിപ്പോർട്ടിൽ വീഴ്ച വന്നാൽ കേസന്വേഷണം പിഴയ്ക്കും. കേസുകൾ വാദിക്കാൻ സൈബർ ജ്ഞാനമുള്ള അഭിഭാഷകർ വേണം. കേസുകൾ വിസ്തരിച്ച് തീർപ്പ് കല്പിക്കാൻ സൈബർ കുറ്റങ്ങളെക്കുറിച്ച് അറിവുള്ള ന്യായാധിപന്മാരും ആവശ്യമാണെന്ന് ജസ്റ്റിസ് പറഞ്ഞു.

സൈബർക്കേസുകൾ കൈകാര്യംചെയ്യാൻ അറിയാവുന്ന 44 അഭിഭാഷകരേ ഇന്ത്യയിലുള്ളൂ. കുറ്റകൃത്യങ്ങളുടെ നിരക്ക് കൂടിയ സാഹചര്യത്തിൽ കൂടുതൽ അഭിഭാഷകരും വേണം.

കോയമ്പത്തൂർ പി.എസ്.ജി. ടാഡിറ്റോറിയത്തിൽ ദേശീയ സൈബർസുരക്ഷാ ഉന്നതതല യോഗത്തിൽ മദിരാശി ഹൈക്കോടതി മുൻ ജഡ്ജി ടി.എൻ. വല്ലിനായകം പ്രസംഗിക്കുന്നു

പ്രത്യേക ഏജൻസി വേണം. കേസുകളും അന്വേഷിക്കാൻ സംസ്ഥാനതലത്തിലും ജില്ലാതലത്തിലും സൈബർക്കേസുകളും കൈകാര്യം ചെയ്യുന്ന പോലീസും കോടതിയും വേണം. കമ്പ്യൂട്ടർ വിജ്ഞാനം പോലുമില്ലാത്ത ജുഡീഷ്യറി ഉദ്യോഗസ്ഥർ ഇത്തരം കേസുകൾ കൈകാര്യം ചെയ്യിട്ട് കാര്യമില്ലെന്നും പരാതിക്കാരന് നിരാശരായി മടങ്ങേണ്ടിവരുമെന്നും ജസ്റ്റിസ് പറഞ്ഞു.

എ.ടി.എമ്മുകളിൽ വ്യാപകകൃത്രിമം നടക്കുന്നുണ്ട്. കമ്പ്യൂട്ടർ വീട്ടുകൊണ്ടും കമ്പ്യൂട്ടർ കൈകാര്യം ചെയ്യുന്നവരുടെ കൈപ്പിഴകൊണ്ടും തെറ്റുപറ്റുന്നത് സ്വാഭാവികമാണ്. ഇതിനെയെല്ലാം തടയുന്ന സൈബർ വിജ്ഞാനം അത്യാവശ്യമായി ബന്ധപ്പെട്ട് പ്രവർത്തിക്കുന്നവർക്ക് നൽകാനും ബന്ധപ്പെടുവർക്ക് കഴിയണമെന്ന് ജസ്റ്റിസ് പറഞ്ഞു.

കോയമ്പത്തൂർ പി.എസ്.ജി. ടാഡിറ്റോറിയത്തിൽ നടന്ന സമ്മേളനത്തിൽ മദിരാശി ഹൈക്കോടതി മുൻ ജഡ്ജി ടി. എൻ. വല്ലിനായകം അധ്യക്ഷത വഹിച്ചു. മുൻ കാബിനറ്റ് സെക്രട്ടറി എസ്. മണ്ഡേന്ദ്രനാഥൻ, ഇളങ്കോവൻ എന്നിവർ പ്രസംഗിച്ചു.

സൈബർ കുറ്റകൃത്യങ്ങളെയും അവ തടയുന്നതിനുവേണ്ട നടപടികളെയുംകുറിച്ച് ടെക്നിക്കൽ സെഷനിൽ കേന്ദ്ര അഡീഷണൽ ചീഫ് സെക്രട്ടറി ഡോ. ജി.എ. രാജകുമാർ പ്രബന്ധം അവതരിപ്പിച്ചു.

സിക്കിം ഗവൺമെന്റ് സ്റ്റോർട്സ് യുവജന കാര്യ പ്രിൻസിപ്പൽ സെക്രട്ടറി ഡോ. കെ. ജയകുമാർ, ജസ്റ്റാസുവ, ലോകേഷ് കുമാർ, സന്തീഷ് അഗർവാൾ, ലോകേഷ് കുമാർ, ഡോ. എസ്. അമർ പ്രസാദ് റെഡ്ഡി, സുഭാഷ് സുനിൽ, ഉമാപതി ചന്ദ്രശേഖർ, കെ. ശ്രീധരൻ, ശങ്കർ വാനവരായർ, അരുൾ ശെൽവർ എന്നിവർ പ്രബന്ധം അവതരിപ്പിച്ചു.

Mathrubhumi Sep 21 Pg 13