RAJASTHAN STATE LEGAL SERVICES AUTHORITY

CYBER CRIME & CYBER LAW AWARENESS

May,2020

NISHEETH DIXIT

ADVOCATE

World Wide Web

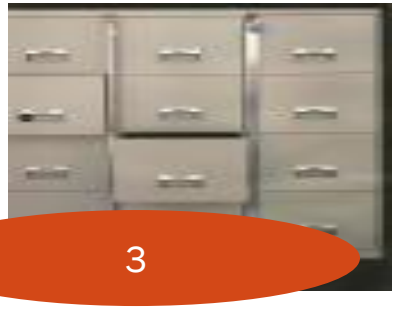
has now become

World Wide Worry

What is cybercrime?

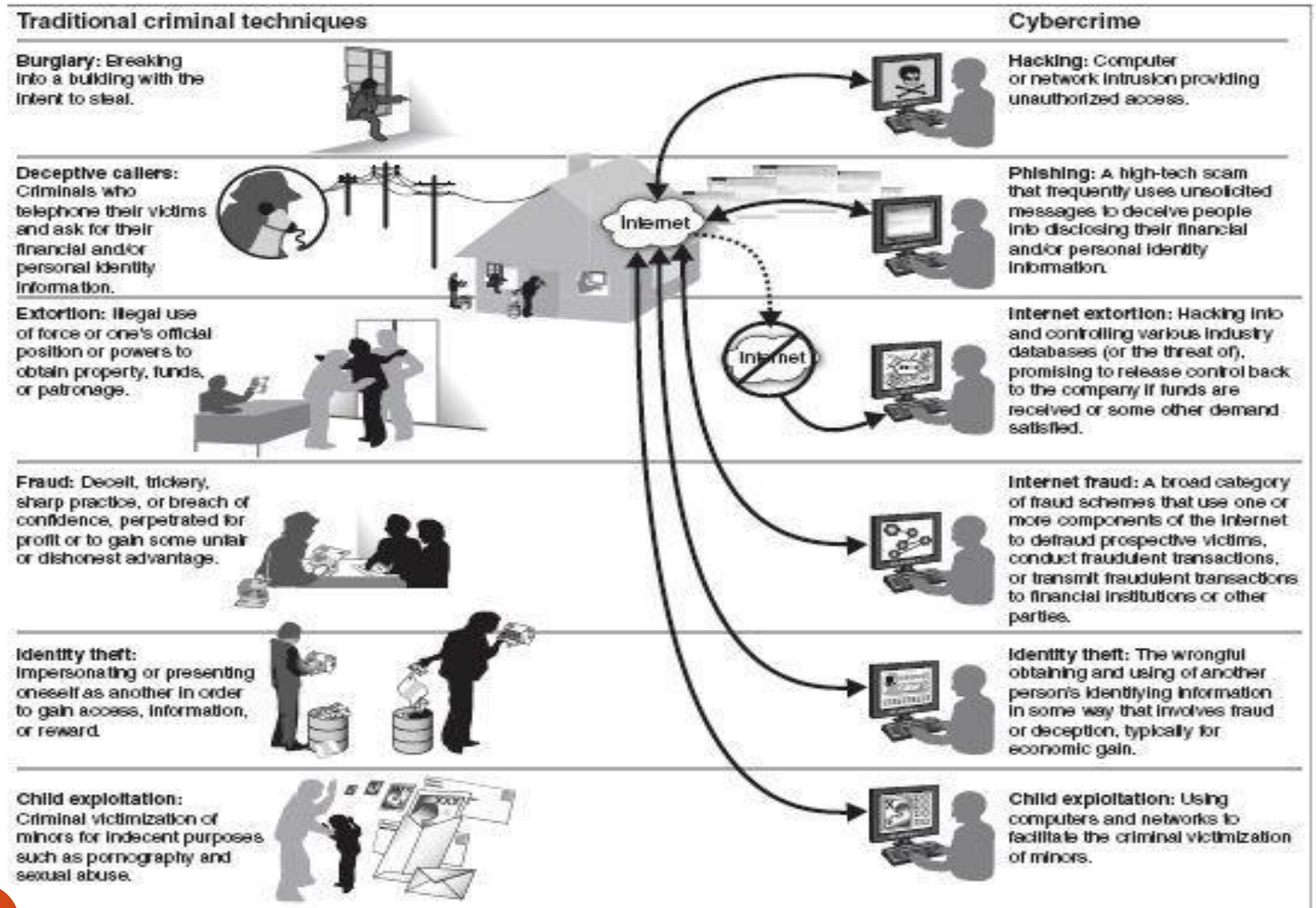
Cybercrimes are divided into 3 categories:

- crimes where a computer is the target of the crime,
- crimes where a computer is a tool of the crime, and
- crimes where a computer is incidental to the commission of the crime.

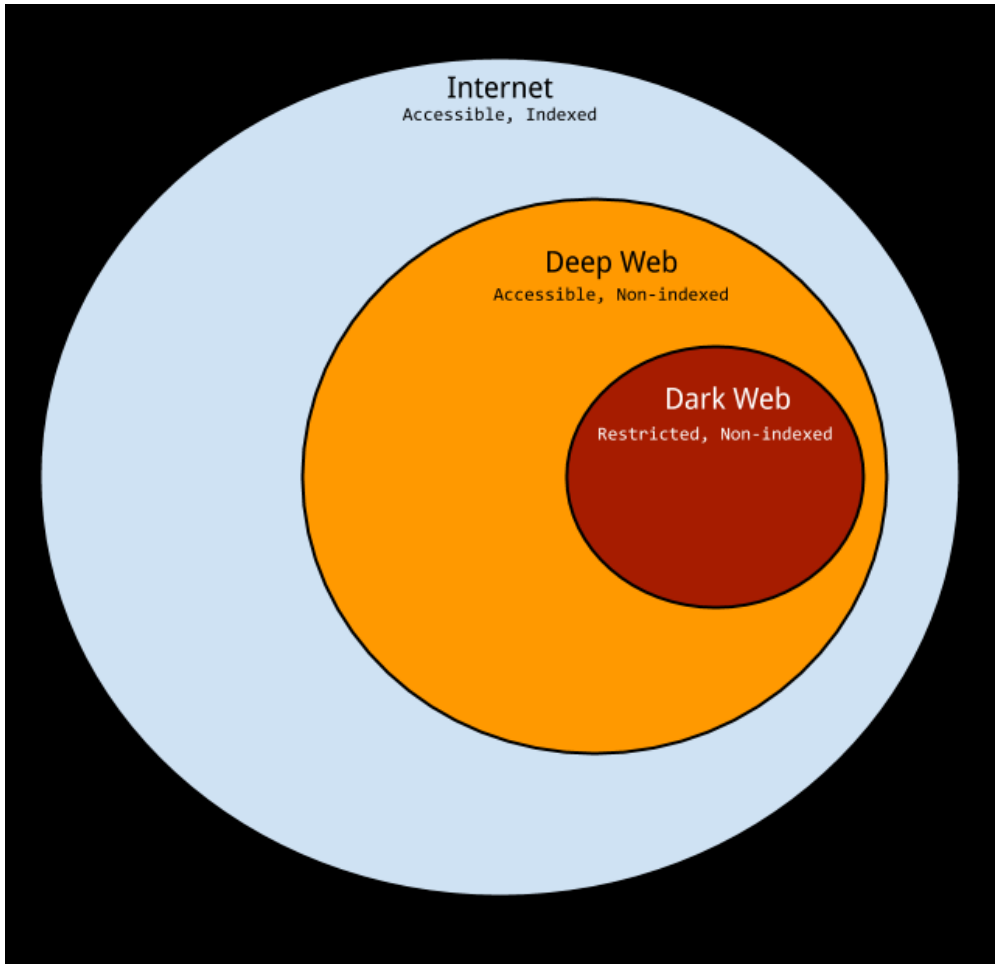


- **Cyber Crime - "Combination of crime and computer Resource".**
- What is Computer resource?

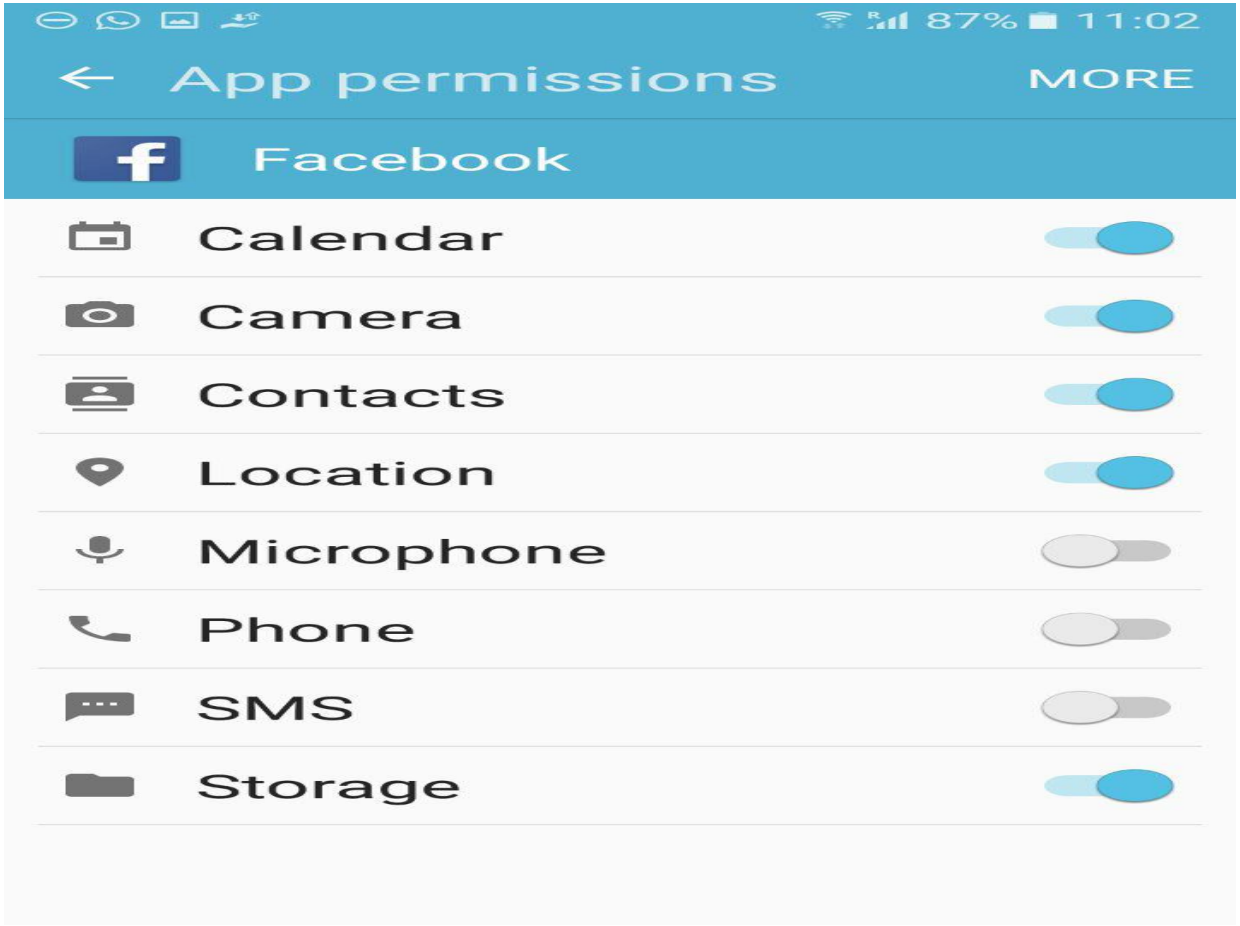
- Cyber crimes are committed while in the cyber space. They include crime like, cyber terrorism, intellectual property infringement, hacking, industrial espionage, on-line child exploitation, internet usage policy abuses ,illegal purchase of goods, sexual assault, internet fraud, software piracy, viruses, impersonation and many more.

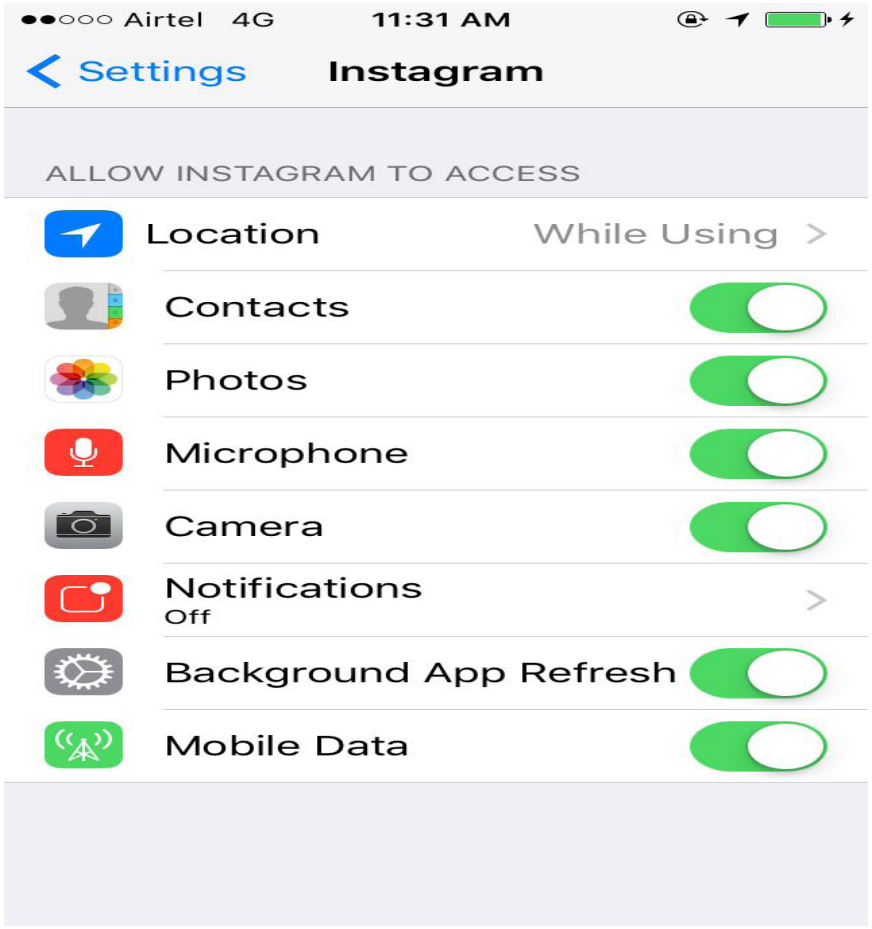

Traditional criminal techniques
Cybercrime
Burglary: Breaking into a building with the intent to steal.
Hacking: Computer or network intrusion providing unauthorized access.
Deceptive callers: Criminals who telephone their victims and ask for their financial and/or personal identity information.
Internet
Phishing: A high-tech scam that frequently uses unsolicited messages to deceive people into disclosing their financial and/or personal identity information.
Extortion: Illegal use of force or one's official position or powers to obtain property, funds, or patronage.
Internet
Internet extortion: Hacking into and controlling various industry databases (or the threat of), promising to release control back to the company if funds are received or some other demand satisfied.
Fraud: Deceit, trickery, sharp practice, or breach of confidence, perpetrated for profit or to gain some unfair or dishonest advantage.
Internet fraud: A broad category of fraud schemes that use one or more components of the Internet to defraud prospective victims, conduct fraudulent transactions, or transmit fraudulent transactions to financial institutions or other parties.
Identity theft: Impersonating or presenting oneself as another in order to gain access, information, or reward.
Identity theft: The wrongful obtaining and using of another person's identifying information in some way that involves fraud or deception, typically for economic gain.
Child exploitation: Criminal victimization of minors for indecent purposes such as pornography and sexual abuse.
Child exploitation: Using computers and networks to facilitate the criminal victimization of minors.

Reasons of Cyber Crime


Internet
Accessible, Indexed
Deep Web
Accessible, Non-indexed
Dark Web
Restricted, Non-indexed

VULNERABILITIES
IN
CYBER SPACE


87% 11:02
App permissions
MORE
Facebook
Calendar
Camera
Contacts
Location
Microphone
Phone
SMS
Storage


●●○○○ Airtel 4G 11:31 AM
Settings
Instagram
ALLOW INSTAGRAM TO ACCESS
Location
While Using
Contacts
Photos
Microphone
Camera
Notifications
Off
Background App Refresh
Mobile Data

web.whatsapp.com

WhatsApp Web

Use WhatsApp on your phone to scan the code

☑ Keep me signed in

To reduce data usage, connect your phone to Wi-Fi

Android
Open WhatsApp — Menu — WhatsApp Web

iPhone
Open WhatsApp - Settings - WhatsApp Web

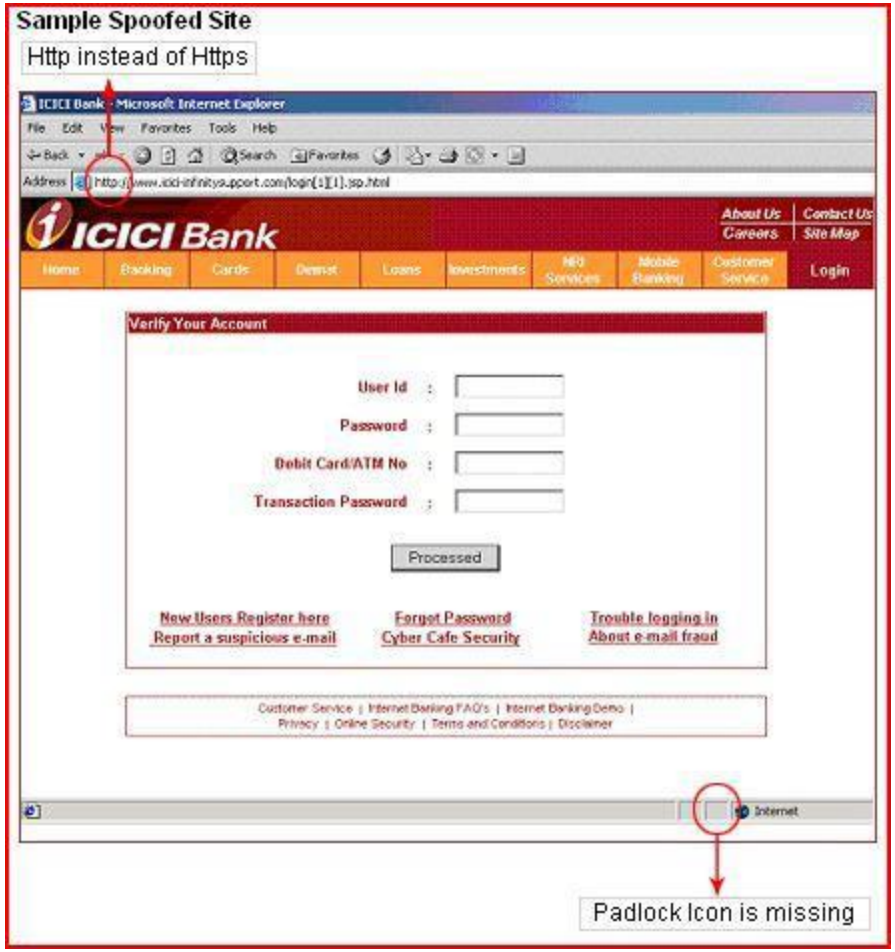
Windows Phone
Open WhatsApp — Menu — WhatsApp Web

BlackBerry
Open WhatsApp — Chats — Menu key — WhatsApp Web

BlackBerry 10
Open WhatsApp — Swipe down from top of screen — WhatsApp Web

Nokia S60
Open WhatsApp — Menu — WhatsApp Web

Nokia S40
Open WhatsApp — Swipe up from bottom of screen — WhatsApp Web


Sample Spoofed Site
Http instead of Https
ICICI Bank - Microsoft Internet Explorer
ICICI Bank
Verify Your Account
User Id :
Password :
Debit Card/ATM No :
Transaction Password :
Processed
New Users Register here
Report a suspicious e-mail
Forgot Password
Cyber Cafe Security
Trouble logging in
About e-mail fraud
Padlock Icon is missing


Camera
Card Skimmer
Keyboard Overlay

Do you often charge your mobile device from public ports while travelling? Did you know this can lead to "**Juice Jacking**" ?


BANK
SECURITY NEWS
52% of cybercrime victims are unable to recover all of the money they lost

CYBER SQUATTING /SPOOFING

Fraudsters use 'duplicate' email to dupe ONGC, Saudi company

MOHAMED THAVER
MUMBAI, OCTOBER 13

IN ONE of the biggest cyber crimes in Mumbai, the Oil and Natural Gas Corporation Limited (ONGC) lost Rs 197 crore after cyber criminals duplicated the public sector firm's official e-mail address with minor changes and used it to convince a Saudi Arabia-based client to transfer payments to their account.

The fraud was committed on the premise that the company making the payment would not notice a minor change in the e-mail address of the ONGC representative, with whom they had been communicating. While ONGC communicated with the company from patel_dv@ongc.co.in, the fraudsters duped the company by communicating with them from patel_dv@ognc.co.in.

According to the BKC cyber police team probing the case, ONGC had an order to deliver 36,000 metric tonnes of Naphtha — flammable liquid hydrocarbon mixtures — to Saudi Aramco, an oil company based in Dhahran. On September 7, ONGC dispatched the order, worth Rs 100.15 crore, from Hazira port in Surat. According to the police, the company usually transferred payments to ONGC's State Bank of India (SBI) account, but did not do so this time.

"ONGC was to send a second batch of naphtha to Aramco on September 22. However, since they had not received the earlier payment, they enquired with the Saudi-based company," an officer said. On being told that the delay was on account of public holidays and bank holidays, ONGC dispatched the second batch of Naptha worth Rs 97 crore on September 22. Again, ONGC e-mailed a scanned copy of the tax invoice with its SBI account number to the company.

Again, no payments were received in the ONGC account. What finally set alarm bells ringing was an e-mail ONGC received on October 7 from Aramco stating that the money had been transferred to a new account. When the PSU contacted Aramco, they were told the company had merely followed up on ONGC's request to deposit the money into an account in Bangkok Bank Public Company Limited. "ONGC had never made such a request," the officer said.

As soon as an official complaint was registered on October 10, Additional Commissioner of Police K M M Prasanna instructed the cyber crime police station to probe the matter on priority. During investigations, police found that someone aware of the e-mail communication between ONGC and Aramco regarding the transfer of a large sum of money had created an e-mail ID similar to an official ONGC email ID.

"The communication from ONGC was done using the e-mail ID patel_dv@ongc.co.in. The fraudsters merely created an e-mail address patel_dv@ognc.co.in," said senior police inspector S Mahadik. Using this ID, the fraudsters began to communicate with Aramco, and as the second email ID appeared almost identical to the original, Aramco officials did not notice the difference. The fraudsters then sent an e-mail asking for the payment to be deposited to a Bangkok-based account. Officers of the BKC cyber police station said an FIR has been registered under Sections 419 (cheating by impersonation), 420 (cheating), 465 (forgery), 468 (forgery for purpose of cheating), 471 (using a forged document) of the Indian Penal Code and Sections 66 C (punishment for identity theft) and D (cheating by impersonation using computer resource) of the Information Technology Act. ONGC was unavailable for comment.

E-MAIL ID TWEAKED

CYBER CRIMINALS duplicated the public sector firm's official e-mail address with minor changes and used it to convince a Saudi Arabia-based client to transfer payments to their account

WHILE ONGC used the ID patel_dv@ongc.co.in to communicate with its client, fraudsters used patel_dv@ognc.co.in

RANSOMWARE


Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT
Payment will be raised on
5/15/2017 16:50:06
Time Left
02:23:34:22
Your files will be lost on
5/19/2017 16:50:06
Time Left
06:23:34:22
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin
ACCEPTED HERE
Send $300 worth of bitcoin to this address:
115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn
Copy
Check Payment
Decrypt

RANSOMWARE

Ransomware is a type of malicious software (malware) that freezes your computer or mobile device until a sum of money is paid. It can destroy personal and business files, leading to stolen data and large financial losses.

KNOW

Ransomware attacks—especially those that target small businesses—**are evolving in complexity and are on the rise.**

All devices are vulnerable, but more and more **mobile attacks** are being reported.

$209 Million collected by criminals in the first quarter of 2016.

A projected **$1 Billion + in losses** from ransomware attacks in 2016 alone, according to the FBI.

Ransom fees vary, from $200 – $10,000.

IDENTIFY

Ransomware targets a specific individual within a business, or a consumer with a link or attachment that infects your computer with malware or leads you to an infected website. Three ways ransomware can take shape are:

Spear phishing emails

- The sender appears to be someone you may know or someone relevant to your business.
- The message is often personalized, and may include your name or a reference to a recent transaction.

Advertisements or pop-up windows

- Your computer freezes, and a popup message appears.
- The message may threaten a loss of your files or information, or may also tell you that your files have been encrypted.

Downloadable Software

- Ransomware is also present in downloadable games and file-sharing applications.

Once the PC is infected, your files are encrypted and inaccessible. The fraudster demands a ransom payment in order to unlock them.

PREVENT

- ☐ **Always back up your files and save them offline or in the cloud.**
- ☐ **Always use antivirus software and a firewall.** Be sure they are set to update automatically.
- ☐ **Enable popup blockers.**
- ☐ **Don't click.** Be cautious when opening emails or attachments you don't recognize—even if the message comes from someone in your contact list.
- ☐ **Only download software from sites you know and trust.**
- ☐ **Alert your local law enforcement agency as soon as you encounter a potential attack.**

American Bankers Association

THE TIMES OF INDIA
CITY

City | Bhopal | Crime | Civic Issues | Politics | Schools & Colleges | Events

News » City News » Bhopal News » Crime » Cards 'cloned' at ATM in Bhopal, 12 people duped

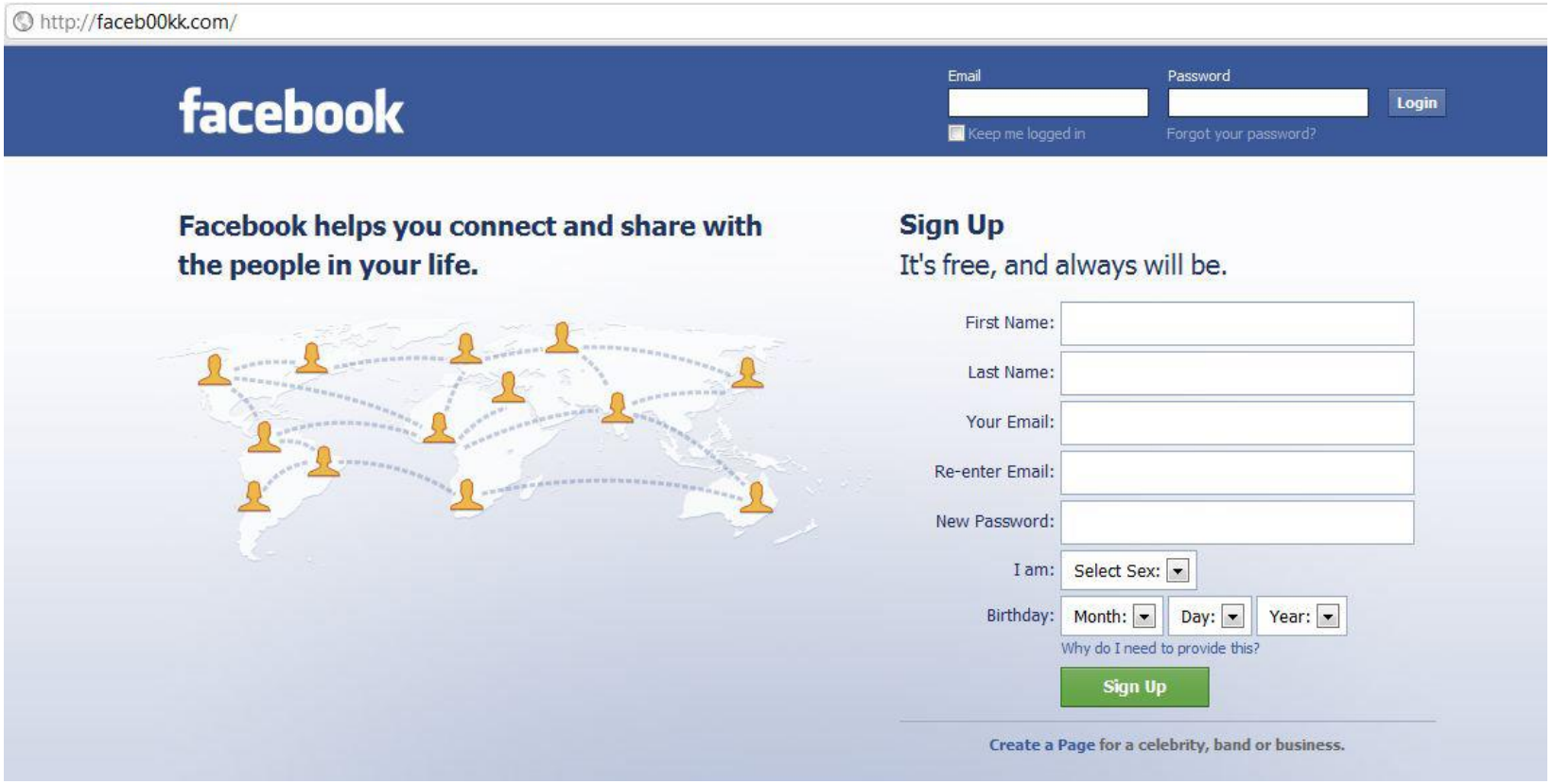
Cards 'cloned' at ATM in Bhopal, 12 people duped

TNN | Updated: Jul 14, 2017, 11:10 AM IST

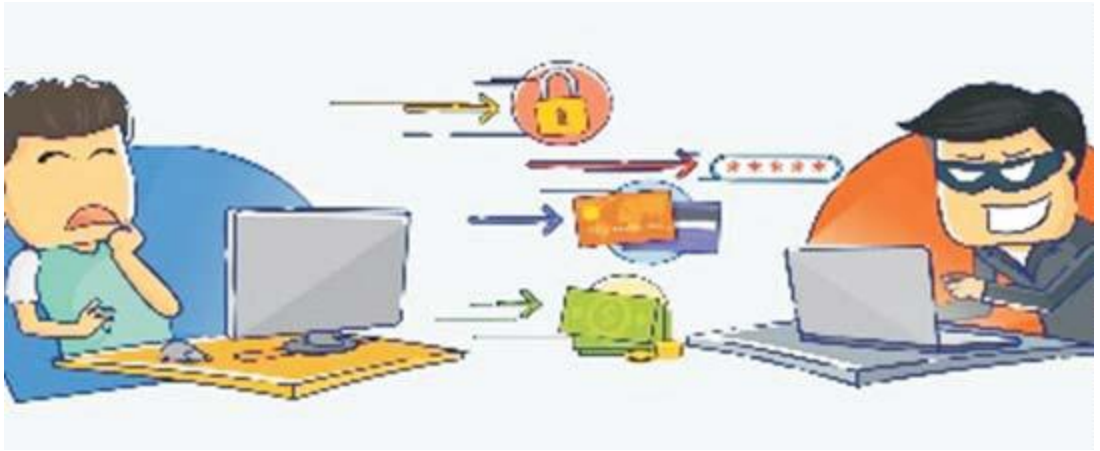
A- A+

Representative image

BHOPAL: It started as a normal day at the cyber cell of Bhopal police. Someone complained that his debit card has been hacked and money withdrawn from his account. Sadly, such news is not uncommon these days. Then came another similar complaint. And another. And soon it was a flood.


http://faceb00kk.com/
facebook
Email
Password
Login
Keep me logged in
Forgot your password?
Facebook helps you connect and share with the people in your life.
Sign Up
It's free, and always will be.
First Name:
Last Name:
Your Email:
Re-enter Email:
New Password:
I am:
Select Sex:
Birthday:
Month:
Day:
Year:
Why do I need to provide this?
Sign Up
Create a Page for a celebrity, band or business.

CYBER CRIMES



- Depending upon the victim of cyber crime, it may be broadly classified under three heads:

  (i) Against individuals;

  (ii)Against Organizations; and

  (iii)Against Society at large.

Against Individuals-Under this category it can be against Individuals or against Individual property through the means of

(a) Harassment via E-mails

(b) Cyber Stalking

(c) Dissemination of obscene material

(d) Defamation

(e) Unauthorized control/access over computer system

(f) Indecent exposure

(g) E-mail spoofing

(h) Cheating and fraud

(i) Computer vandalism

(j) Transmitting virus

(k) Net trespass

(l) IPR crimes

(m) Internet time thefts

(n) Sextortion…

Against Organizations-Against organizations it can be through the means of :

(a) Unauthorized control/access of computer system

(b) Possession of unauthorized information

(c) Cyber terrorism against the government organization

(d) Distribution of pirated software etc..

Against Society at large Under this category it can be through:

(a) Pornography & child pornography

(b) Polluting the youth through indecent exposure

(c) Trafficking

(d) Financial crimes

(e) Sale of illegal articles

(f) Online gambling

(g) Forgery

DIFFERENT TYPES OF CYBER CRIMES

Cyber crime is an evil having its origin in the growing dependence on computers in modern life. The following are computer related crimes(cyber crimes):-

- **Financial crime**-This would include cheating, credit card fraud, money laundering etc..Internet offers certain unique advantages which no other medium has like anonymity and speed. The internet also offers a global marketplace for consumers and business. These factors together work up to make up a haven for any fraudulent activities online.

- Various Internet frauds include online auctions, Internet access services, work-at-home plans, travel/vacations, advance fee loan, prizes, lotteries etc.
- Credit and debit card fraud.
- Safety Tips

PSYCHOLOGICAL TRICKS-PHISHING

- **PHISHING-**
- This is the criminal practice of using voice over phones systems to gain access to details about account numbers, PIN, date of birth and expiry date of credit card holders and using it for fraudulent activities.
- Phishing, Vishing and Smishing are done in an attempt to steal money from the victim or cause any other harm to the victim.

- **Lottery Fraud**
- **Job Related Fraud**
- **Matrimonial Fraud**
- **Case Studies & Safety Tips**

- **Sale of illegal articles**-This would include sale of narcotics , weapons and wildlife etc. by posting information on websites , bulletin board or simple by using e-mail communications.
- **Online gambling**-There are millions of websites, all hosted on servers abroad, that offer online gambling. They are fronts for money laundering.(The world of online gambling due to its anonymity, unfortunately has many other hazards like danger of illegal use of credit card or illegal access to bank account.
- **Intellectual property crimes-** These includes Copyright infringement, trademark violation, patent violation, domain name registration, software piracy.
- **Software piracy**-These include software piracy, copyright infringement, trademarks violations, theft of computer source code etc.
- **Cybersquatting.**
- Typosquatting
- Case Studies & Safety Tips

- **Cyber defamation**-This occurs when defamation takes place with the help of computers and or the internet example- someone published defamatory matter about someone to all of that person's friends.

- **Corporate Cybersmear** –It is a false and disparaging rumor about a company, its management or its stock that is posted on the Internet. This kind of criminal activity has been a concern specially in stock market and financial sectors where knowledge and information are the key factors for businessmen.
- Case Studies & Safety Tips

- **Hacking or unauthorized access to computer system or network**-Hacking means unauthorized attempts to by pass the security mechanisms of an information system or network. Hacking of protected system is punishable under sec-70 (IT Act,2000)
- Black hat, White hat and Grey hat- Hackers and Crackers
- **Kinds of hackers-**
- **Code hackers**-They can make the computer do nearby anything they want it to.
- **Crackers-They** break into computer systems .Circumventing Operating Systems and their security is their favorite pastime.
- **Cyberpunks**-They are the masters of cryptography
- **Phreakers**-They combine their in-depth knowledge of the Internet the mass telecommuications system.

- **Theft of information contained in E-form-** This includes theft of information stored in computer hard disks, removable storage media, etc.
- **E-mail bombing-This** refers to sending a large amount of e-mails to the victim resulting in the victim's e-mail account or mail server crash.
- **Data didling-** This kind of attack involves altering the raw data just before it is processed by a computer and then changing it back after the processing is completed.
- Case Studies

Computer viruses are small software programs that are designed to spread from one computer to another and to interfere with computer operation. A virus might corrupt or delete data on your computer, use your e-mail program to spread itself to other computers, or even erase everything on your hard disk.

- **Salami attacks-** These attacks are used for the commission of financial crimes. The key here is to make the alteration so insignificant that in a single case it would go completely unnoticed.

  Example-bank employee inserts a program into bank's servers that deducts a small amount from the account of every customer.

- **Denial of service attack**-This involves flooding customer resource with more request than it can handle. This causes the resources to crash thereby denying authorized users the service offered by the resources.

- **Trojan**-This is an unauthorized program which functions from inside what seems to be an authorized program thereby concealing what is actually doing. It is a malicious, security-breaking program that is disguised as something benign, such as directory lister, archiver, game, or a program to find and destroy viruses. A special case of Trojan Horses is the ***mockingbird***-software that intercepts communications(especially login transactions) between users and hosts and provides system-like responses to the users while saving their responses(especially account IDs and passwords)

- Case Studies & Safety Tips

- **Key loggers**-Key logger is a software programme or a device designed to secretly monitor and log all key stores. The key logger software scan computers, their processes and data, the moment a person strikes a key on the keyboard, This information is immediately carried over to an external controller.
- **Identity theft**-This involves pretending to be someone else in order to steal money or get other benefits .The identity of another individual is impersonated in order to commit credit card fraud, create false profits at networking sites and operate false e-mails. Identities.
- **Website defacement-** This is usually carried out by the substitution of the homepage of a site by a system cracker that breaks into a web server and alters the hosted website creating one of its own. The hacker usually replaces the site matters with his own message or completely destroy the sites.
- Case Studies

Spoofing

- SMS
- Call
- Email

- **Steganography**
- It is the process of hiding one message or file inside another message or file. It is "the art of writing in cipher, or in characters which are not intelligible except to persons who have the key ;cryptography".
- Steganographers can hide an image inside another image, an audio or video file, or they can hide an audio or video file inside another media file, or even inside a large graphic file. Steganography differs from cryptography in that while cryptography works to mask the content of a message, stenography works to mask the very existence of the message.
- Micro-dots

DIFFERENT TYPES OF CYBER FRAUDS

- Banking Fraud
- Bit coin MLM frauds
- Fraud to get government benefits
- Counterfeiting of currency
- Creation of false companies
- False advertising
- False billing
- False insurance claims & Franchise Fraud
- Investment Frauds Marriage Fraud
- Tax Fraud..

SOCIAL MEDIA FRAUDS

- **Social Media Frauds?**
- Social Media has become an integral part of our lives. It is the new way of communicating, sharing and informing people about the events in our lives. We share our day to day lives on social media in the form of self and family photographs, updates on our locations/whereabouts, our views/thoughts on prevalent topics etc. One can understand the entire history of an individual through their social media profile and can even predict future events based on patterns in the past.
- **Sympathy Fraud**
- **Romance Fraud**
- **Cyber Stalking**
- **Cyber Bullying**

Bank ATM & OTP frauds

ONLINE BANKING FRAUDS

- **Digital Payments Applications related attacks**
- **SIM Swap case**
- **OTP Frauds**
- **Hacking of Bank Account due to Weak Password**
- **Hacking of Multiple Accounts due to same password**

- DEBIT CARD CLONING
- Debit Card skimming happens when the PIN is revealed to another person. A scamster who knows the PIN and has possession of the card even for a short while can replicate the card with a skimming device and withdraw cash.
- Shoulder Surfing
- POS Machines
- Cinema, Malls and other places.

- GENERAL SAFETY TIPS

- Always keep your systems/devices (desktop, laptop, mobile) updated with latest patches.
- Protect systems/devices through security software such as anti-virus with the latest version.
- Always download software or applications from known trusted sources only. Never use pirated software on your systems/devices.
- Ensure all devices/accounts are protected by a different strong PIN or passcode. Never share your PIN or password with anyone.
- Do not share your net-banking password, One Time Password (OTP), ATM or phone banking PIN, CVV number etc. with any person even if he/she claims to be an employee or a representative of the bank and report such instances to your bank.
- Always change the default admin password on your Wi-Fi router to a strong password known only to you. In addition, always configure your wireless network to use the latest encryption (contact your network service provider, in case of any doubt).
- Be cautions while browsing through a public Wi-Fi and avoid logging in to personal & professional accounts such as e-mail or banking on these networks.
- Always use virtual keyboard to access net-banking facility from public computers; and logout from banking portal/website after completion of online transaction. Also ensure to delete browsing history from web browser (Internet Explorer, Chrome, Firefox etc.) after completion of online banking activity.

- Do scan all e-mail attachments for viruses before opening them. Avoid downloading e-mail attachments received in e-mails from unknown or un-trusted sources.
- Be careful while sharing identity proof documents especially if you cannot verify the authenticity of the company/person with whom you are sharing information.
- Note the IMEI code of your cell phone and keep it in a safe place. The operator can blacklist/ block/trace a phone using the IMEI code, in case the cell phone is stolen.
- Observe your surroundings for skimmers or people observing your PIN before using an ATM.
- Discuss safe internet practices and netiquettes with your friends and family regularly! Motivate them to learn more about cybercrimes and safe cyber practices.
- Do not save your card or bank account details in your e-wallet as it increases the risk of theft or fraudulent transactions in case of a security breach.
- If you think you are compromised, inform authorities immediately.

- **Password/Passphrase-**
- **Password may be a single word but a** combination of more words would be a Passphrase. A Passphrase is more secured than a Password. Since you are being asked to create the Passwords, use all that is available on a keyboard to create one. Change it often. Use different passwords for different accounts and devices
- Preventions: Passwords having a dictionary meaning are easy to crack.
- You are the creator of your own destiny thus create a complex password that is also easy to remember thereby safeguarding your online destiny.
- Never Share it with anyone Ever.

CRIME AGAINST WOMEN & CHILDREN

Cyber bulling

- **Cyber Bullying:**
- **Sending tormenting post, harassing messages,** threatening contents to a minor to cause mental harassment and depressive or suicidal state of mind to the recipient of such messages.
- Preventions: Share those messages and posts with your Parents or teachers who are matured enough to understand the gravity of the matter and act accordingly. Do not keep on facing or enduring these troubles.

- **PHOTO EDITING APPS**
- **These apps that you use to beautify yourself are** also known to retain your original copy of the photo you have uploaded and even the copy of the edited version is saved on their servers. You can only wonder what next would they do with the copy of your photos!
- Preventions: Use reputed apps that you should be downloading from secured App stores. The fake photo editors may cause you harm and edit your lifestyle if used by them with criminal intent.

- **CLICK WRAP CONTRACTS**

- **'I accept', 'I agree': It is easy to accept the terms and conditions** before downloading that app or software or game or e-book or music or video that you want it on your digital devices. But before that, understand at what cost are you giving permissions!
- Preventions: 'Look before you Leap' and so 'Read before you Tread' just before hitting on the 'I accept' or 'I agree' tab.

- MOBILE RECHARGE SHOP
- A Mobile Recharge Shop is a place where scamsters can gain access to your cellphone number because you have provided it to the recharge vendor.
- This number is then misused to call or text you and exploit your ignorance or even emotionally manipulate you.

- KEYLOGGER
- It is a malicious program that may be installed in the victim's computer for recording computer user keystrokes to steal passwords and other sensitive information. With Keylogger a scamster will be able to collect login details and other matter saved in the computer and have them mailed to a designated email address.

- CYBER STALKING
- Cyber stalking is the use of the Internet or other electronic means to stalk or harass another by misusing information uploaded on social networking sites.
- CALL SPOOFING
- Call spoofing happens through apps that enable a person with criminal intent to change one's number and voice to impersonate another to defraud the receiver.

- CAMERA HACKING
- Camera hacking happens when photographs of a person are taken without consent, through malware that got downloaded with an attachment.
- Phones with no camera guard can be exploited for such criminal activities.

- **VOYEURISM**
- **Privacy breach is biggest concern with advent of pin** hole cameras and latest spy cams that can be hidden and are not easily detectable. Could be hidden in shopping malls, changing rooms, washrooms, hospitals and diagnostic centers, and also in offices and washrooms located in private offices.

- PROFILE HACKING
- Profile Hacking happens when your email or social networking site is accessed by a probable stalker who then compromises it.

- PICTURE MORPHING
- Morphing the face of a person to the body of another and publishing it to blackmail or otherwise intimidate the person is one of the ways by which people who upload photos on social networking sites can be exploited.

- ONLINE GAMES
- Girls who are vulnerable to loneliness, low self esteem and clinical depression can fall prey to dangerous online games that may become addictive and further harm them. Some like the notorious blue whale challenge even end in the victim ending her life. This is a personal as well as social challenge for the others around.
- JOB CALL LETTER
- Websites offering jobs need to be checked for veracity and authenticity. Mails need to be double checked and verified before one responds and acts on instructions provided, especially if one is asked to put in a personal appearance.

- DEEPFAKES
- Deepfake is a technique that is used to combine and superimpose new images and videos onto source images or videos. It is used to create videos where the voice or face of another is superimposed on the original in such a way that the viewer or listener cannot distinguish or doubt the veracity of it.

- **Report if you find content related to of Child Pornography (CP)/Child Sexual Abuse Material (CSAM) or sexually explicit material**
- Any content related to of Child Pornography (CP)/ Child Sexual Abuse Material (CSAM) or sexually explicit material such as Rape/ Gang Rape (CP/RGR) content should be report to the concerned social media website
- If anybody of your acquaintance shares Child Pornography (CP)/ Child Sexual Abuse Material (CSAM) or sexually explicit material with you, it is your duty as a responsible citizen to inform the concerned person that publication, collection and distribution of Child Pornography (CP)/ Child Sexual Abuse Material (CSAM) or sexually explicit material is illegal and he should refrain from doing such activities.
- You can also report it on National Cyber Crime Reporting Portal (www.cybercrime.gov.in)

- **How to deal with Child Pornography (CP)/ Child Sexual Abuse Material (CSAM) or sexually explicit material in workplace?**
- All organizations should have clear and strong HR policies on how to deal with content on Child Pornography (CP)/ Child Sexual Abuse Material (CSAM) or sexually explicit material
- Organizations should have clear rules for use of electronic devices provided by the organisation
- If any employee is found possessing obscene or indecent content, proper investigation and action should be taken against them
- The organisation should report any incidence of sharing and storage of obscene content within the organisation to the police. The copy of the content should be saved as an evidence with restricted access
- All other copies of the content should be deleted
- They can also report through National Cyber Crime Reporting Portal (www.cybercrime.gov.in).

- **Publication, Collection and Distribution of Child Pornography (CP)/Child Sexual Abuse Material (CSAM) or sexually explicit material is illegal**
- Under Section 67 and 67A of Information Technology Act, 2000 makes publication and distribution of any material containing sexually explicit act or conduct in electronic form a punishable offence
- Section 67B of IT Act, criminalizes browsing, downloading, creation, publication and distribution of child pornography (Obscene and Indecent representation)
- POCSO Act Amendment.

- SOCIAL TROLLING
- Social Trolling is posting inflammatory messages or visuals about a person or organisation in an online community with the express purpose of causing humiliation or nuisance to the object of trolling.

- COVID-19 –Social Media cases
- Hate Speech
- Rumors
- Defamation
- Disobey of Public order
- Case Studies

SAFETY TIPS

COMPUTER EMERGENCY RESPONSE TEAM –INDIA (CERT-IN)

- All organizations providing digital services have been mandated to report cyber security incidents to CERT-In expeditiously.
- Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre) has been launched for providing detection of malicious programmes and free tools to remove such programmes.
- Issue of alerts and advisories regarding cyber threats and counter-measures by CERT-In.
- Issue of guidelines for Chief Information Security Officers (CISOs) regarding their key roles and responsibilities for securing applications / infrastructure and compliance.
- Provision for audit of the government websites and applications prior to their hosting, and thereafter at regular intervals.
- Empanelment of security auditing organisations to support and audit implementation of Information Security Best Practices.
- Formulation of Crisis Management Plan for countering cyber attacks and cyber terrorism.
- Conducting cyber security mock drills and exercises regularly to enable assessment of cyber security posture and preparedness of organizations in Government and critical sectors.
- Conducting regular training programmes for network / system administrators and Chief Information Security Officers (CISOs) of Government and critical sector organisations regarding securing the IT infrastructure and mitigating cyber attacks.

SAFETY TIPS FOR USING E-MAIL

- Avoid exposure of E-Mail account details such as user name and password to unknown /unauthorized persons while using E-Mail.
- Avoid unauthorised disclosure of email contents to protect privacy of information
- Avoid clicking of web-links provided in email messages to prevent secretly installation of a malware (e.g., virus) on your computer
- Install latest Anti-virus/Anti-Spyware software and keep them up-to-date.
- Install personnel (Desktop/user level) Firewall on the system.
- Keep Operating System and application software updated with latest security updates / patches in the computer system used for email to prevent the exploitation of the weakness in the system.
- Be suspicious while opening unexpected emails.
- Do not open suspicious email Attachments.

- Scan an email attachment before opening/downloading to minimize the risk of downloading malware (e.g., virus).
- Use encryption for sending and receiving confidential email to ensure that message can only be read by the intended recipients.
- Do not respond suspicious/banking-related (Phishing)/ winning lottery / fund transfer emails to avoid becoming a victim of financial frauds.
- Do not open untrusted/unknown emails (spam)
- Enable spam filter to reduce amount of spam/junk emails
- Keep strong password with minimum of Eight characters, comprising a combination of alphabets (both upper and lowercase), numbers and special characters.
- Do not keep your computer unattended to avoid misuse

Video Conferencing

- **Require Passwords:** As a meeting host, this is the No. 1 action that you can take to secure your meetings: Make passwords mandatory for all your meetings to protect against uninvited guests and to secure information about the meeting, including meeting name and organizer.

- **Verify Attendees:** Be sure to check the attendee list when sending out the meeting invitation, and review the participants list during the call. Remove anyone on the call who is not supposed to be a part of the meeting. For meetings where confidential information is being shared, such as a company all-hands meeting, increase security by requiring participants to authenticate by logging in before they can join the meeting.

- **Check Meeting Links:** When you receive a meeting invitation, verify that it's from a known, trusted sender. Also, check the meeting link before clicking, watching out for malicious links with ".exe," for example. There's a steep rise in phishing attempts where malicious links have the names of video conferencing vendors embedded but they take you to phony login sites. By using password-embedded links, you will increase security and reduce war dialing, a technique used to discover or guess the meeting ID.

- **Patching**: Make sure your video conferencing software is patched with the latest vendor-provided updates and have automated upgrades turned on.

- **Keep Confidentiality:** Keep confidential conversations private, and be sure you're not accidentally sharing anything confidential on your laptop or in your background. Virtual backgrounds have gained popularity for a change of scenery!

- **Review Your Security Settings:** Review and enable appropriate security and privacy settings to prevent threat actors from exploiting known vulnerabilities.

- **Keep Kids Secure:** As kids are connecting via video conferencing for school and other activities, parents can help them do so securely and teach them how to be safe online. Talk to kids about not chatting with strangers or giving out private and personal information.

- **Report Suspicious Activity:** Remember to report any suspicious activity to your corporate Information Security and Information Technology teams. If you are using an external video conferencing technology for non-work related calls, reach out to the vendor for the best way to report suspicious activities

LEGAL REMEDIES

- RBI Guidelines-06.07.2017
- cybercrime.gov.in

- Civil cases-
- IT Adjudication
- Consumer Cases

- Criminal Cases-
- Complaint
- FIR

INFORMATION TECHNOLOGY ACT, 2000 & AMENDMENT 2008

- **Information Technology Amendment Act 2008** was placed in the Parliament and passed at the end of 2008 (just after Mumbai terrorist attack of 26 November 2008 had taken place). The IT Amendment Act 2008 got the President assent on 5 Feb 2009 and was made effective from 27 October 2009.

- **Main features of the ITAA 2008 are:**
  - Focusing on data privacy
  - Focusing on Information Security
  - Defining cyber café
  - Making digital signature technology neutral
  - Defining reasonable security practices to be followed by corporate
  - Redefining the role of intermediaries
  - Recognizing the role of Indian Computer Emergency Response Team
  - Inclusion of some additional cyber crimes like child pornography and cyber terrorism
  - Not Below the rank of Inspector shall investigate IT Act matters

Cyber Contraventions

- A cyber contravention refers to a civil wrong under IT Act, 2000.It is important to note that Law of torts provide remedies for civil wrong where affected person can compel the wrong doer to pay damages by way of compensation. However, for cyber contravention damages are provided under sec-43-45 of IT Act,2000.

- **Section 43 – Penalty and Compensation for damage to computer , computer system**

  If any person without permission of the owner or any other person who is in-charge of a computer, computer system or computer network –

  a. Accesses or secures access to such computer, computer system or computer network or computer resource

  b. Downloads, copies or extracts any data, computer data, computer database or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium

  c. Introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network

  d. Damages or causes to be damaged any computer, computer system or computer network, data, computer database, or any other programmes residing in such computer, computer system or computer network-

  e. Disrupts or causes disruption of any computer, computer system, or computer network;

  f. Denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means

g Provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made there under

h. Charges the services availed of by a person to the account of another person by tampering with or manipulating any computer of a computer, computer system or computer network

I Destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means,(2008 Amend)

J Steals, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage,(2008 Amend)

- he shall be liable to pay damages by way of compensation to the person so affected

- **Sec-43A-Compensation for failure to protect sensitive personal data**

  Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resources, which it owns, controls, or operates is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person.

- Then such body corporate shall be liable to pay damages by way of compensation to the person so affected.
- (Rules 2011)

Cyber-IT Act crimes

- Tampering with computer source Documents Sec.65
- Computer related offences -Sec.66
- Dishonestly receiving stolen computer resource or communication device(Sec- 66B)
- Identity theft Sec.66C
- Cheating by personation by using computer resource Sec.66D
- Violation of body privacy Sec.66E
- Cyber terrorism Sec.66F
- Publishing or transmitting obscene material in electronic form Sec .67
- Publishing or transmitting of material containing sexually explicit act, etc. in electronic form Sec.67A
- Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic formSec.67B

- Preservation and Retention of information by intermediaries Sec.67C
- Powers to issue directions for interception or monitoring or decryption of any information through any computer resource Sec.69
- Power to issue directions for blocking for public access of any information through any computer resource Sec.69A
- Power to authorize to monitor and collect traffic data or information through any computer resource for Cyber Security Sec.69B
- Un-authorized access to protected system Sec.70
- Penalty for misrepresentation Sec.71
- Breach of confidentiality and privacy Sec.72
- Punishment for Disclosure of information in breach of lawful contract Sec72A
- Publishing False digital signature certificates Sec.73
- Publication for fraudulent purpose Sec.74

- Act to apply for offence or contraventions committed outside India Sec.75
- Compensation, penalties or confiscation not to interfere with other punishment Sec.77
- Compounding of Offences Sec.77A
- Offences with three years imprisonment to be cognizable Sec.77B
- Exemption from liability of intermediary in certain cases Sec.79
- Examiner of Electronic Evidence
- Punishment for abetment of offences Sec.84B
- Punishment for attempt to commit offences Sec.84C
- Offences by Companies Sec.85

STAY SAFE, BROWSE SAFE

T H A N K S

RAJASTHAN STATE LEGAL SERVICES AUTHORITY

&

NISHEETH DIXIT

ADVOCATE

9829112511