CYBER CRIMES & CYBER LAWS

NISHEETH DIXIT

ADVOCATE

LL.M-Cybercrimes & Cyber Laws, MBA (HR)

MSc. –Cyber Forensics & Information Security

- **Cyber criminology** is defined as "the study of causation of crimes that occur in the cyberspace and its impact in the physical space.

- The term CYBERSPACE literally means 'navigable space' and Cyber is derived from the Greek word *kyber* (to navigate).

I. **HOW MANY CYBER ATTACKS HAPPEN PER DAY IN 2022?:**

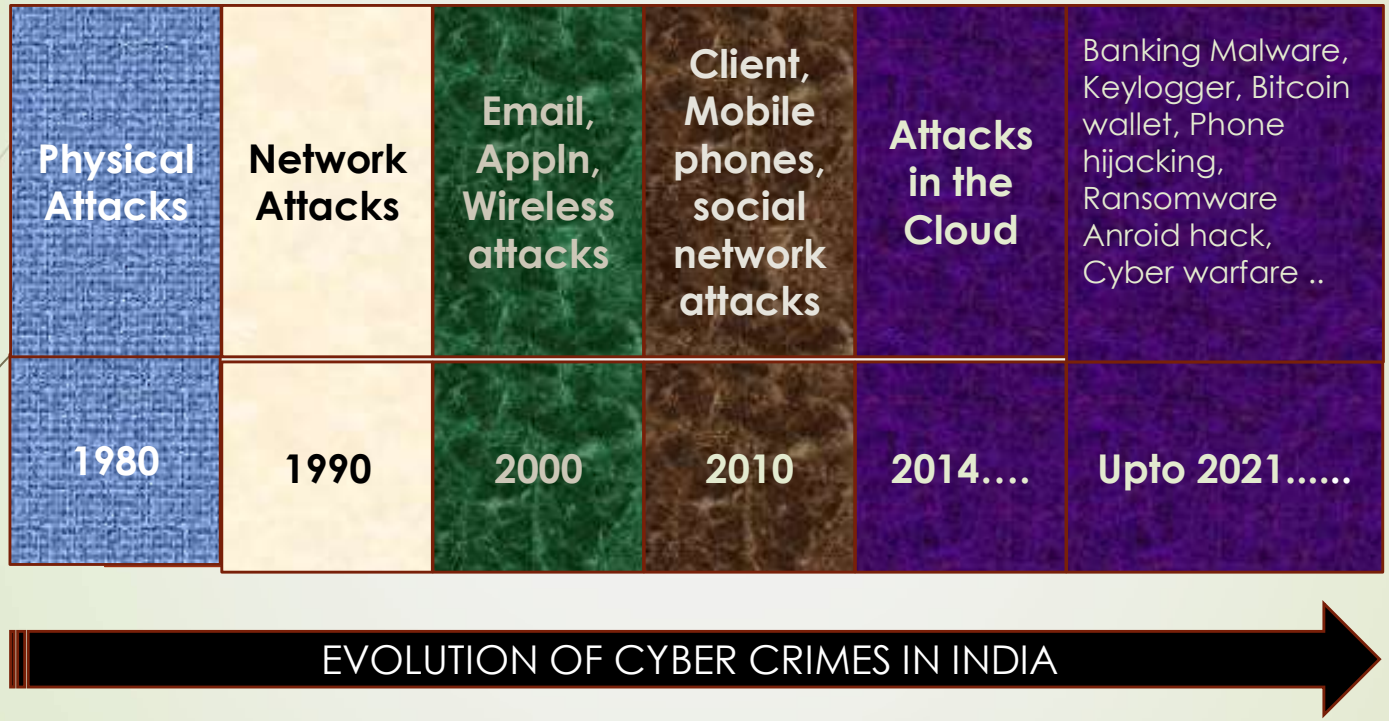
II. **ARE WE READY TO COMBAT CYBER ATTACKS?**

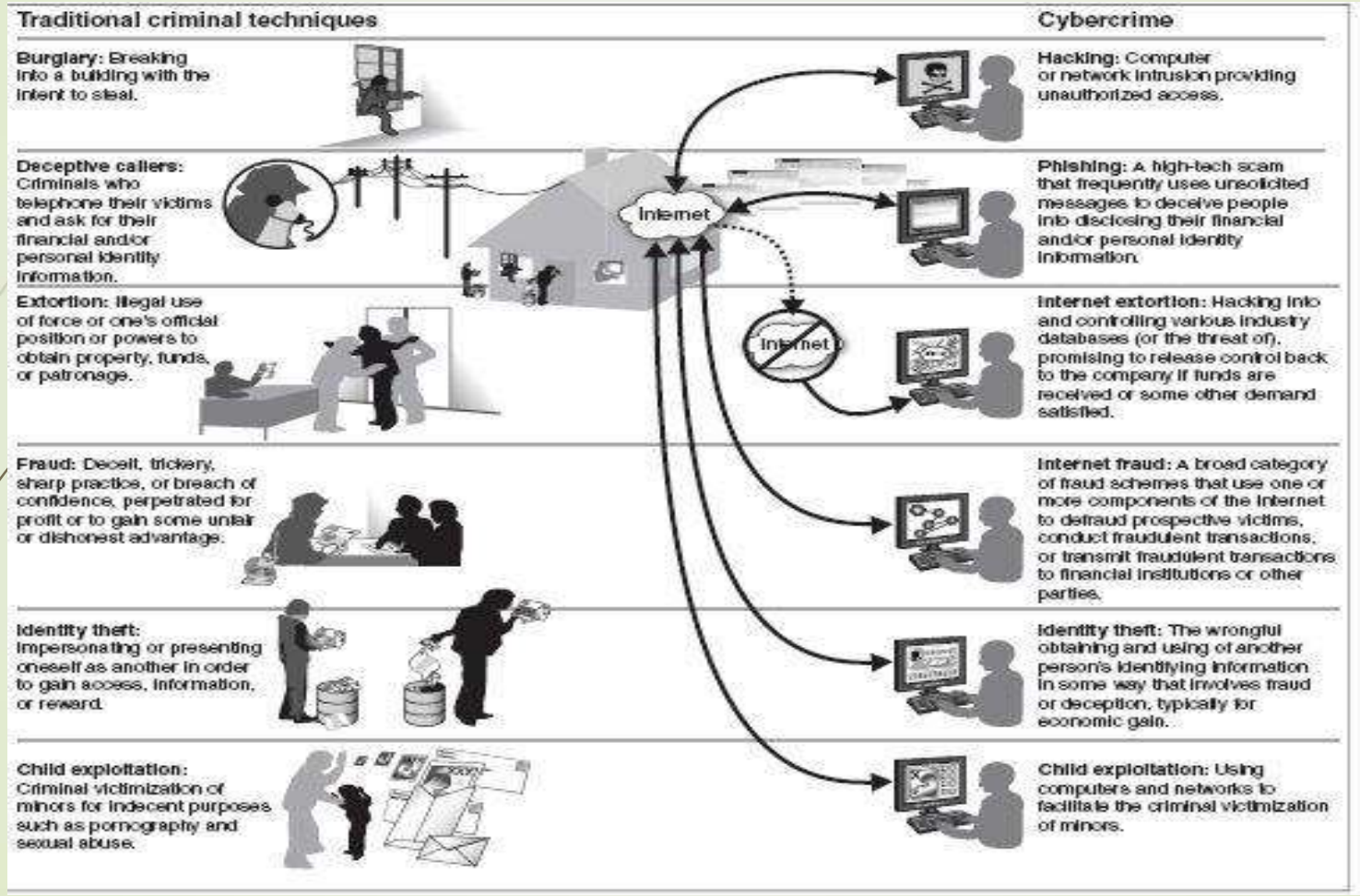
- Globally, **30,000 websites** are hacked daily.
- **64% of companies** worldwide have experienced at least one form of a cyber-attack.
- In 2020, ransomware cases grew by **150%**.
- Email is responsible for around **94% of all malware**.
- **Every 39 seconds,** there is a new attack somewhere on the web.
- An average of **around 24,000 malicious mobile apps** are blocked daily on the internet.

CYBER CRIME

Cyber crime is a term used to broadly describe criminal activity in which computers or computer networks are a tool, a target or a place of criminal activity and include everything from electronic cracking to denial of service attacks.

- 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.


Physical Attacks
Network Attacks
Email, Appln, Wireless attacks
Client, Mobile phones, social network attacks
Attacks in the Cloud
Banking Malware, Keylogger, Bitcoin wallet, Phone hijacking, Ransomware Anroid hack, Cyber warfare ..
1980
1990
2000
2010
2014....
Upto 2021.....
EVOLUTION OF CYBER CRIMES IN INDIA


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.

Classification

a) Data crimes include –

(i) data interception (an attacker monitors data streams to or from a target in order to gather information),

(ii)data modification (interception of data in transit and modification of parts of that data before retransmitting it)and

(iii)data theft (illegal copy or theft of data from a business or other individual).

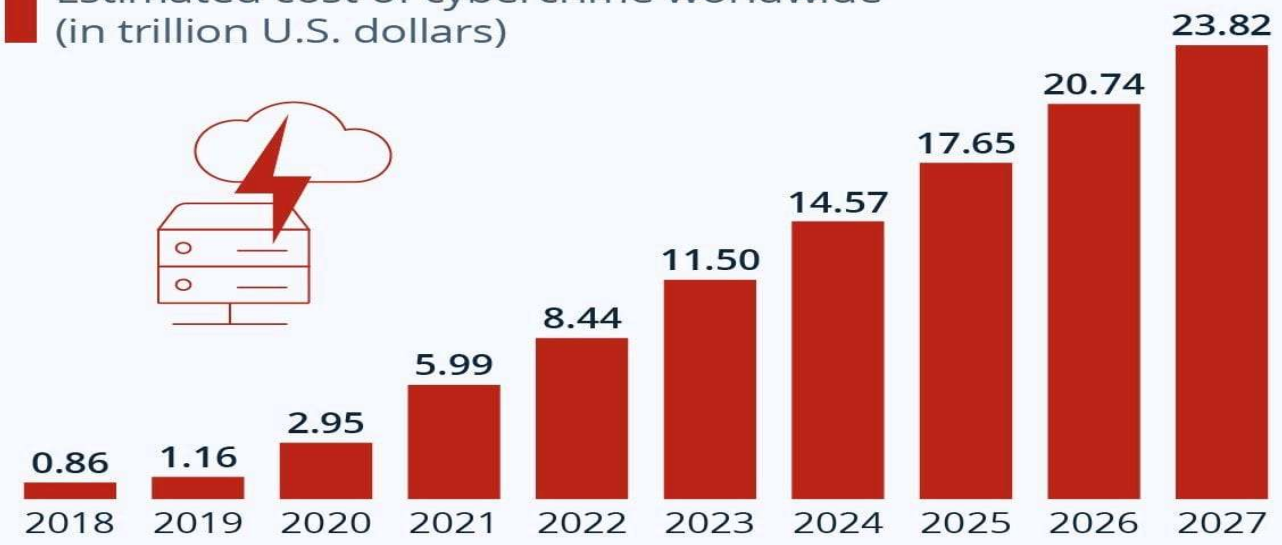
b)Network crimes enclose interfering with the functions of a computer network by inputting, transmitting, damaging, modifying or suppressing network data.

c)Access crimes refer to unauthorized access and virus dissemination.

d) Content-related crimes such as violations of copyright, unsolicited commercial messaging, and cyber threats

Cybercrime Expected To Skyrocket in the Coming Years

Estimated cost of cybercrime worldwide
(in trillion U.S. dollars)



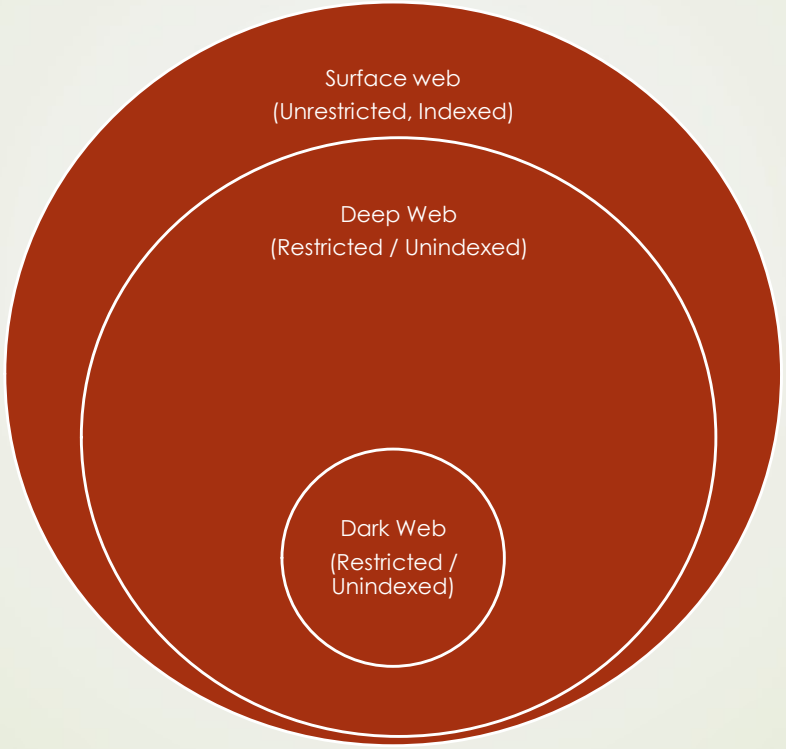
As of November 2022. Data shown is using current exchange rates.
Sources: Statista Technology Market Outlook,
National Cyber Security Organizations, FBI, IMF

statista

CYBER CRIMINALS

Reasons of Cyber Crime

World Wide Web

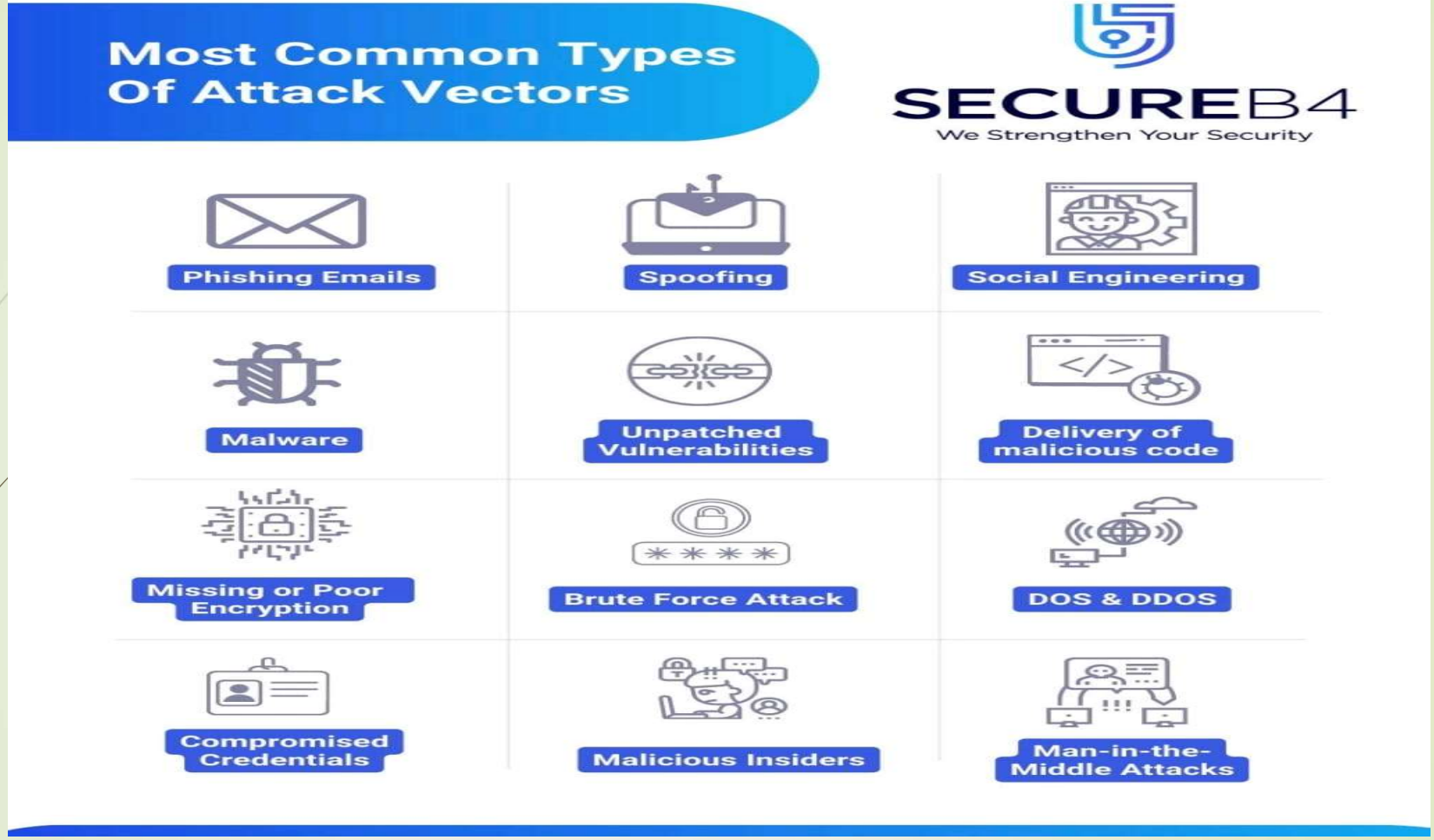


- **Internet / WWW**
  - Surface Web
  - Deep Web
  - Dark Web
- **Deep Web:**
  - Internet content which is either not, or cannot be, indexed by usual search engines
  - dynamic web pages
  - blocked sites
  - unlinked sites
  - private sites
  - non-HTML content
  - contextual content
  - scripted content
  - limited-access networks
- **Dark Nets (Anonymous Networks)**
  - The Onion Router (TOR) Project
  - Invisible Internet Project (I2P)
  - Free Net, etc.

VULNERABILITIES IN CYBER SPACE

Most Common Types Of Attack Vectors

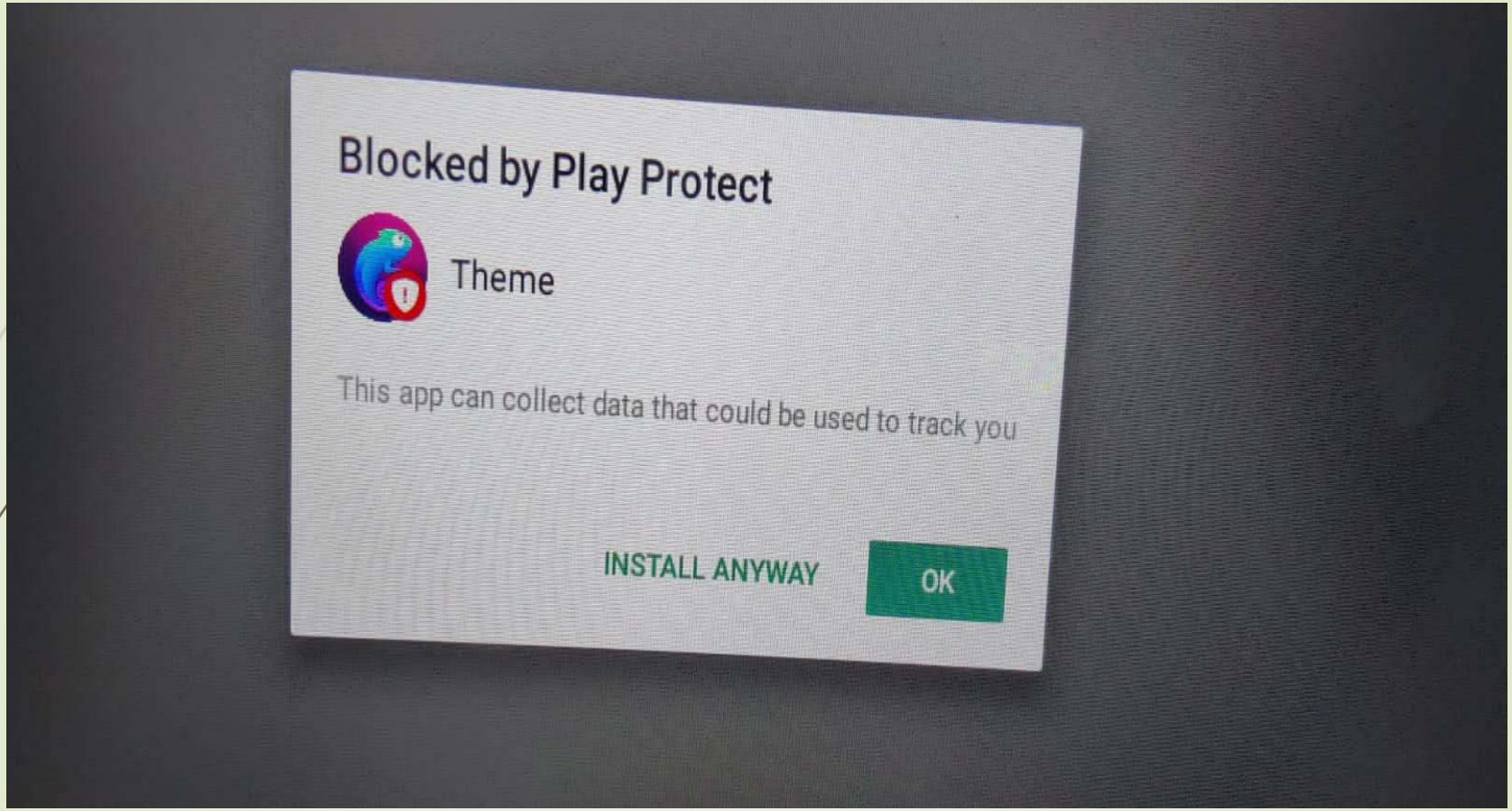
SECUREB4
We Strengthen Your Security

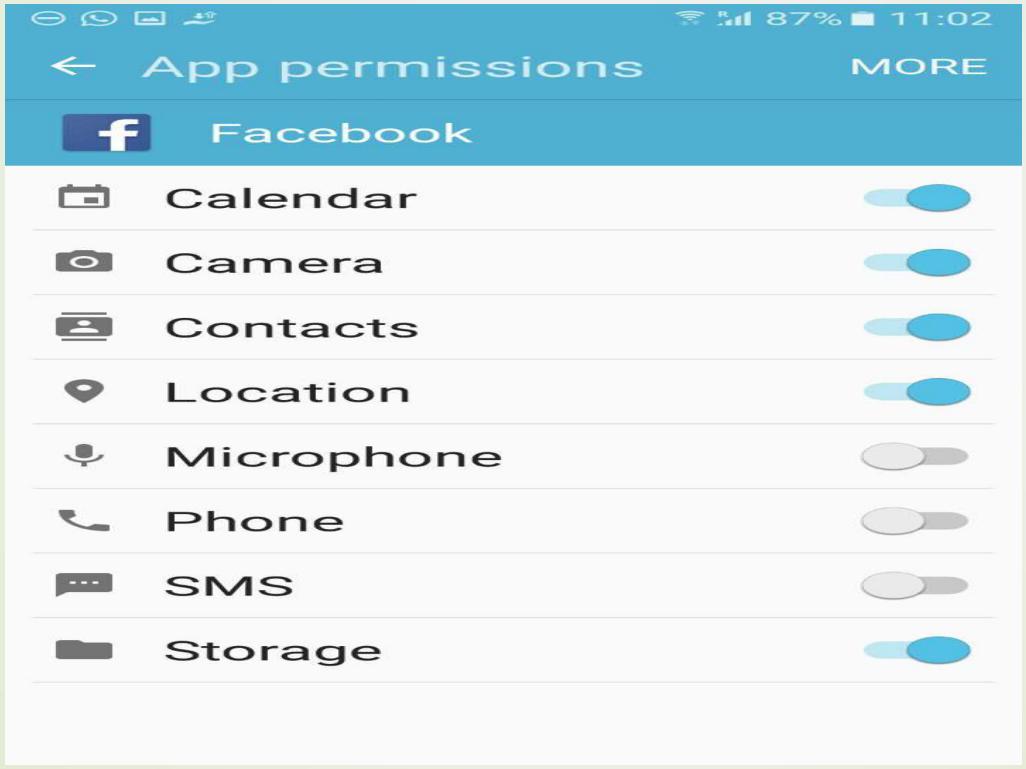


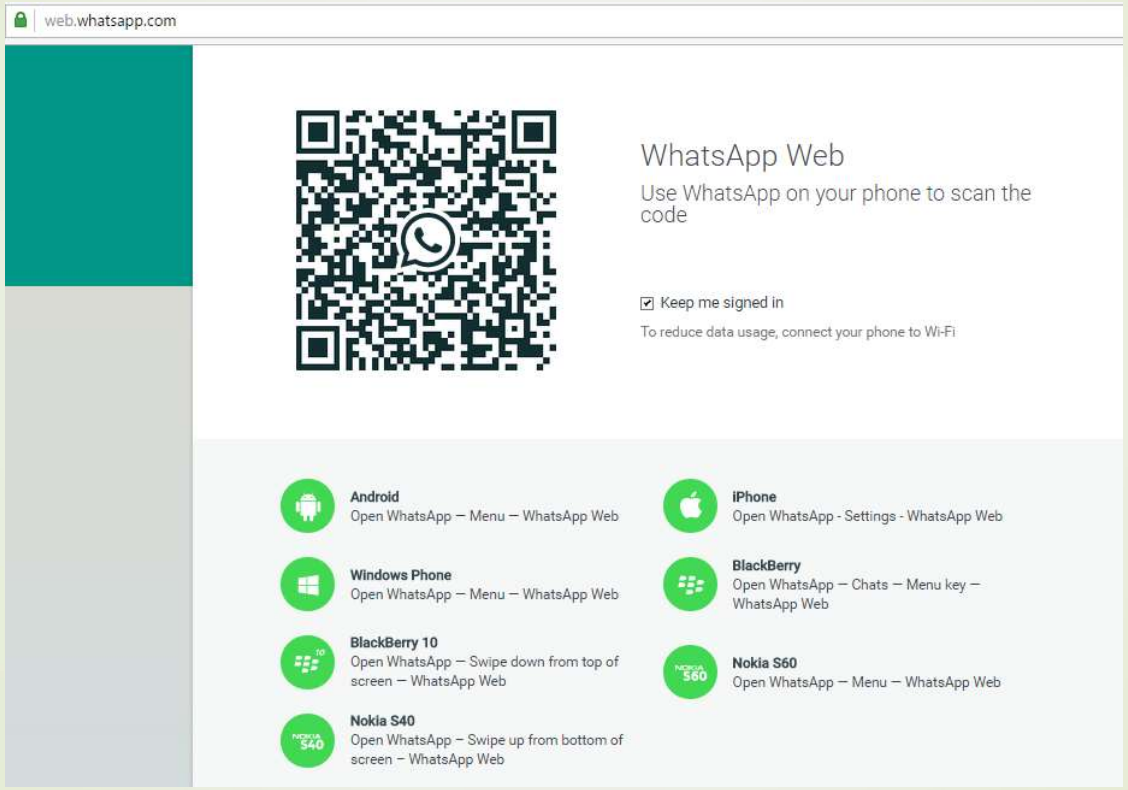
10 Common Cybersecurity Gaps That Leave Organizations Vulnerable

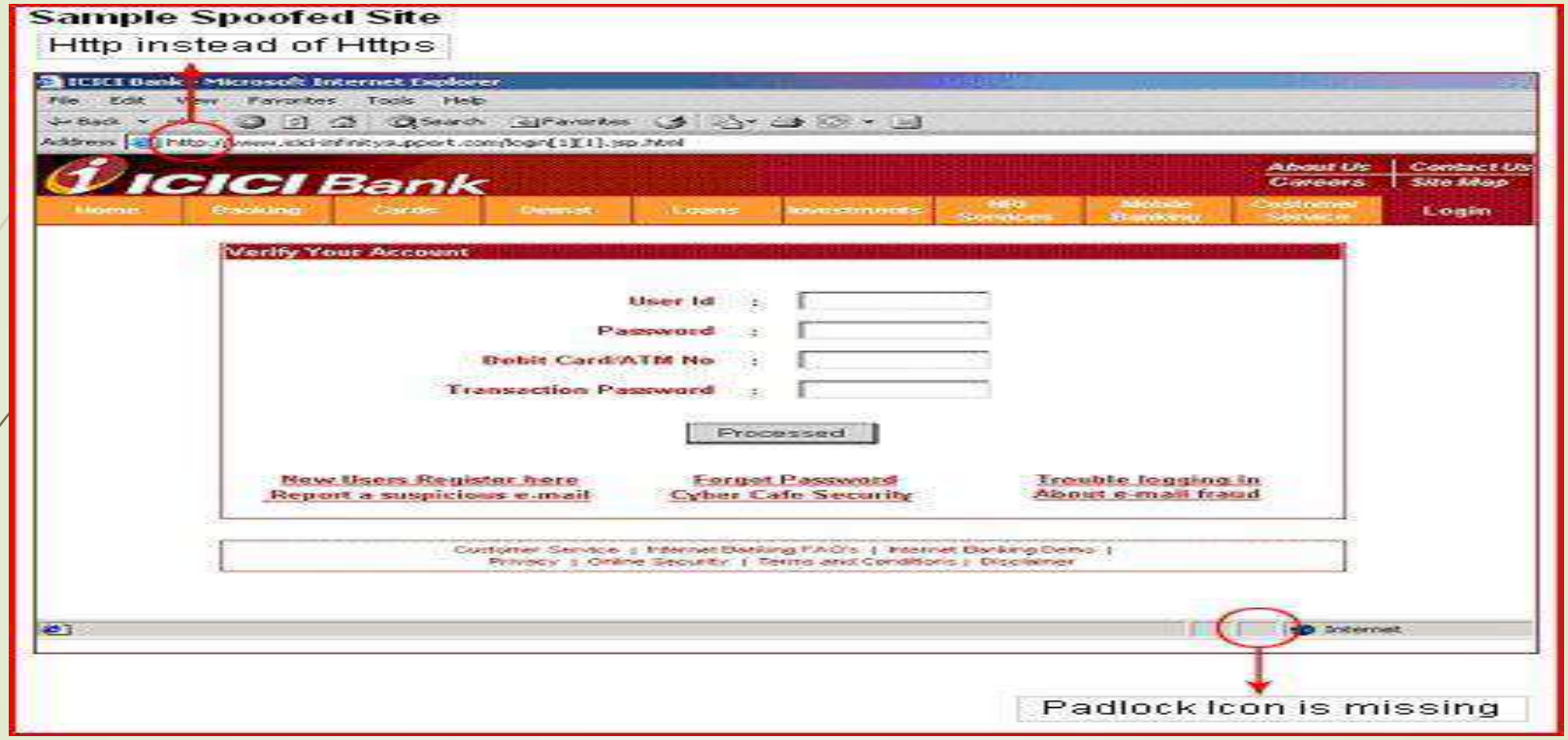
SECURE
We Strengthen Your Se

- Lack of Security Awareness Training
- Inadequate Cybersecurity Policies and Procedures
- Unpatched Software and Operating Systems
- Weak and Reused Passwords
- Lack of Multi-Factor Authentication
- Poorly Configured Firewalls
- Unsecured Wireless Networks
- Unencrypted Data
- Lack of Backup and Disaster Recovery Plans
- No Security Monitoring and Reporting


Blocked by Play Protect
Theme
This app can collect data that could be used to track you
INSTALL ANYWAY
OK


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


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
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

ND CYBERLAW

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

Beware of Juice Jacking

Attackers use USB charging ports available at public places to install malware, steal data or even take complete control of your device.

Tips to stay safe

- Disable data transfer feature on your mobile phone while charging
- Get a charge only cable instead of cable supporting charging and data transfer capabilities
- Try to carry a power bank
- If possible, switch off the device while charging from public ports


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

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(AIIMS)

THE TIMES OF INDIA
CITY

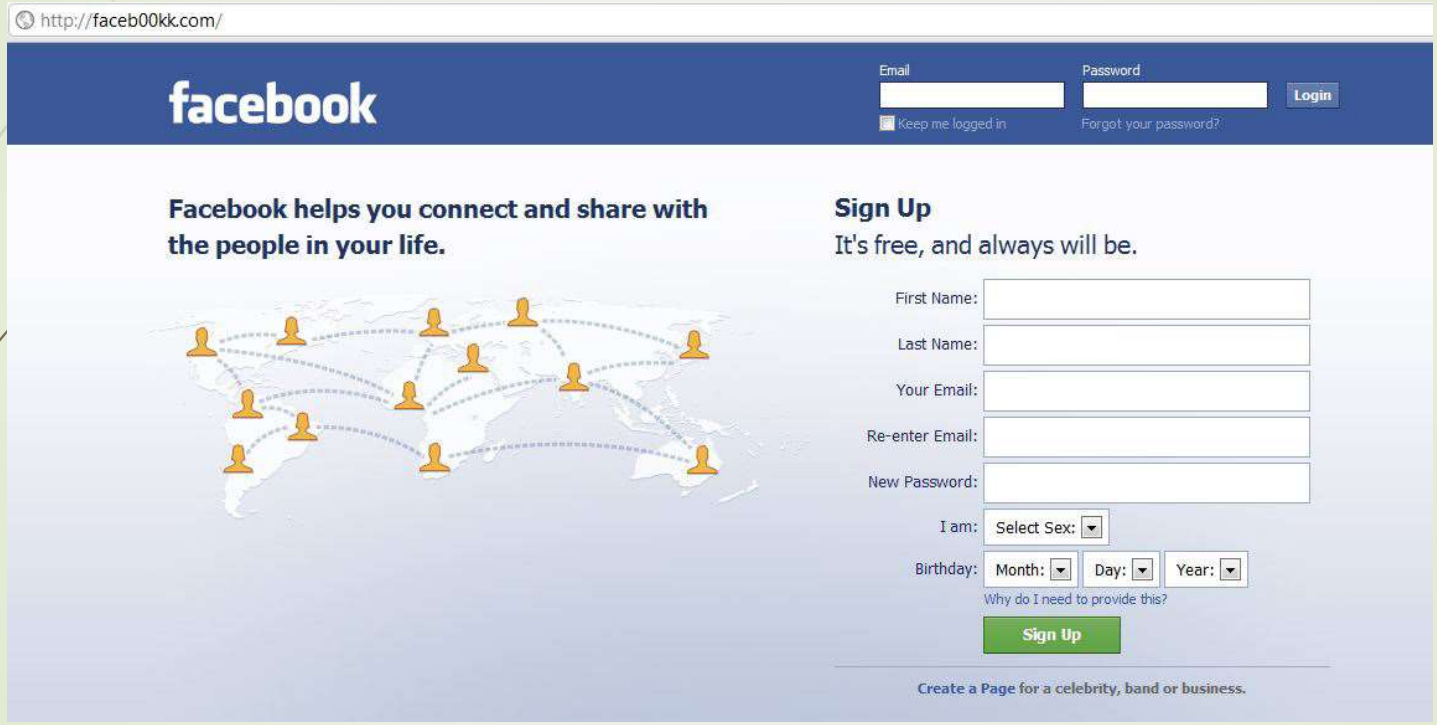
Cards 'cloned' at ATM in Bhopal, 12 people duped

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.

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.

PSYCHOLOGICAL TRICKS-PHISHING

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 Kill 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 Him

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**

CRIME AGAINST CHILDREN

- **Enactment**

  -Child Marriage Restraint Act, the Child Labour (Prohibition and Regulation) Act, 1986
  -Criminal Law (Sexual Offences and Related Matters) Amendment Act, 2007
  -Goa Children's Act, 2003
  -Immoral Traffic (Prevention) Act, 1986
  -Sexual Offenses Act, 2003
  -The Criminal Procedure Code, 1973
  -The Indian Penal Code, 1860
  -The Juvenile Justice (Care and Protection of Children) Act, 2000
  -The Protection of Children from Sexual Offences Act, 2012

  -The Information Technology Act 2000(ITAA 2008)

- **Current forms of child online abuse and exploitation include:**
- **Cyberbullying:** emotional harassment, defamation and social exposure, intimidation, Social exclusion
- **Online sexual abuse:** distribution of sexually explicit and violent content, sexual harassment**(Child Pornography)**
- **Online sexual exploitation:** production, distribution and use of child sexual abuse material (CSAM) (child pornography), “sextortion”, “revenge pornography”
- **Cyber extremism:** ideological indoctrination and recruitment, threats of extreme violence
- **Online commercial fraud:** identity theft, phishing, hacking, financial fraud
- **Habit formation and online enticement to illegal behaviours:** access to alcohol, cheating, plagiarism, gambling, drug trafficking, sexting and self-exposure
- **Grooming:** preparing a child, significant adults and the environment for sexual abuse and exploitation or ideological manipulation

CASE STUDY –ORGANIZATION

Indian Attacks

- Electricity Grid of India Soon to be Insulated from Cyber Attacks Source: https://economictimes.indiatimes.com/
- Union Power Minister Sh. RK Singh has said that India's power network soon would be more future-ready and insulated from cyber-attacks with the provision of routine inspections and timely action under the Electricity Amendment Bill. The power ministry has made a provision for inspecting the national electricity grid in order to maintain cyber hygiene in the network through the Electricity Amendment Bill 2022. The bill provides for amending section 26 of the Act so as to strengthen the functioning of the National Load Despatch Centre (NLDC) for ensuring the grid's safety and security and for the economic and efficient operation of the nation's power system

Cyber Attack on AIIMS New Delhi

- Source: hindustantimes.com, indiatoday.in, business-standard.com.
- All India Institute of Medical Sciences (AIIMS) New Delhi was hit by ransomware on 23rd November 2022. The staff was unable to access the mainstay hospital management application called e Hospital. The patient care services in emergency, inpatient, outpatient and laboratory wings were managed manually after the server went down. Experts from India's Computer Emergency Response Team (Cert-In) examined the affected servers and on 24 November found that four servers (two application servers, one database server and one back-up server), were infected leading to multiple databases being encrypted.
- All infected servers were disconnected by the National Informatics Centre (NIC) team, which manages the eHospital system, to avoid further contamination of other servers. It was found that the firewall deployed to protect the AIIMS network was not properly configured. After more than two weeks the data was retrieved from an unaffected backup server and most of hospital services were restored.
- The Indian Computer Emergency Response Team, Delhi cybercrime special cell, Indian Cybercrime Coordination Centre, Intelligence Bureau, Central Bureau of Investigation (CBI), National Forensic Sciences University, National Critical Information Infrastructure Protection Centre and NIA, among others, were part of the investigation team

- OIL Duliajan Ransomware Attack

Oil India Limited (OIL) headquarters at Duliajan (Assam) was hit by cyberattack on 10 April 2022. A multiagency quick response team including officials from NCIIPC and CERT-In were sent to investigate the incident. The anonymous hackers had demanded a ransom of $7.5 million (57 crore rupees) from OIL to restore the network. The drilling and production operations were normally functioning and the communication network was not affected due to the presence of alternate network of computers.

The data was isolated from the infected servers and is safe.

Cosmos Bank Case

A CASE STUDY

Upcoming challenges

- Metaverse-
- The metaverse can be defined as a simulated digital environment that uses augmented reality (AR), virtual reality (VR), and blockchain, along with concepts from social media, to create spaces for rich user interaction mimicking the real world.
- The major reasons for the need of legislations in the metaverse are as follows:
- ***Metaverse and Data Protection***
- ***Metaverse and IPR***
- ***Metaverse and Digital Harrasment***

IOT-IOMT-IOFT-IOET

- **Crypto Currency Crime**
- Crypto Currency Fraud
- Crypto Currency Theft
- Crypto Currency Scam
- Fraudulent Crypto Exchange
- Fraudulent Crypto Trading Company
- Extortion / Blackmail
- Stock / Share Fraud
- Other

- CYBER SECURITY –CHALLENGES & AWARENESS

10 Ways To Prevent Insider Threats

See something, say something

Encouraging employees to report fishy behavior they have witnessed among their colleagues because all employees are a vital component of a company's security posture.

Educating employees

This will help prevent an accidental breach of security. However, it will not help prevent an intentional data breach.

User access hygiene

This means that all user accounts should be evaluated. All dormant and orphaned accounts should be deleted from the system—for instance, temporary accounts may be created for purposes of a given project that may provide users with access to sensitive data.

Strong authentication

Weak authentication procedures just help attackers infiltrate the system. The system should require employees to use strong passwords as well as multi-factor authentication (MFA) to safeguard their user accounts.

Third-party access

Control third parties such as vendors, contractors, and consultants whenever they are accessing the company's facilities.

Sentiment analysis

This refers to the use of behavioral analysis techniques to handle potential threats.

Compromised accounts

An organization should invest in the detection of compromised accounts. Compromise may result from actions such as malware downloads.

Data exfiltration

Monitoring data and access to data within a company's servers should help prevent successful attacks from insiders.

Monitoring user behavior

The monitoring of employees is the first and most obvious means of protecting the system from possibly threatening a company's informational assets.

Privileged access abuse

Tools that monitor privileged access users and control changes to sensitive information will help reveal efforts to abuse privileges and hence reveal possible attacks.

Hackercombat.com

HACKER COMBAT COMMUNITY

20 Ways to Block Mobile Attacks

Don't let your guard down just because you're on a mobile device. Be just as careful as you would on a desktop!

WiFi

- Don't allow your device to auto-join unfamiliar networks.
- Always turn off WiFi when you aren't using it or don't need it.
- Never send sensitive information over WiFi unless you're absolutely sure it's a secure network.

Apps

- Only use apps available in your device's official store - NEVER download from a browser.
- Be wary of apps from unknown developers or those with limited/bad reviews.
- Keep them updated to ensure they have the latest security.
- If they're no longer supported by your store, just delete!
- Don't grant administrator, or excessive privileges to apps unless you truly trust them.

Browser

- Watch out for ads, giveaways and contests that seem too good to be true. Often these lead to phishing sites that appear to be legit.
- Pay close attention to URLs. These are harder to verify on mobile screens but it's worth the effort.
- Never save your login information when you're using a web browser.

Bluetooth

- Disable automatic Bluetooth pairing.
- Always turn it off when you don't need it.

Smishing (phishing via SMS)

- Don't trust messages that attempt to get you to reveal any personal information
- Beware of similar tactics in platforms like What's App, Facebook Messenger Instagram, etc.
- Treat messages the same way you would treat email, always think before you click!

Vishing (voice phishing)

- Do not respond to telephone or email requests for personal financial information. If you are concerned, call the financial institution directly, using the phone number that appears on the back of your credit card or on your monthly statement.
- Never click on a link in an unsolicited commercial email.
- Speak only with live people when providing account information, and **only** when you initiate the call.
- Install software that can tell you whether you are on a secure or fake website.

KnowBe4
Human error. Conquered.


ABCs of Information Security Awareness
A
Always Properly Logout After Completion of Online Transaction
B
Be Careful What You Click
C
Clear Cookies and Delete Browsing History at the End of Session and Stay Safe
D
Do not Carry Your PIN Number in Wallets Better to Memorize Your PIN
E
Enlighten Yourself On Cyber Security Measures
F
Following Basic Rules of Social Networking Can Prevent Damaging Your Online Relationships
G
Giving Out Your Personal Information Online is not Advisable
H
Help Yourself to Maintain a Positive Online Presence
I
Install Anti-virus Protection
J
Join Hands to Stop Spreading Fake News
K
Keep Software Up to Date
L
Lock Your Devices When Not in Use
M
Monitor Your Account for Any Suspicious Activity
N
Never Believe On Forward Messages, Check Source And URL
O
Only Install Apps and Software From Trusted Sources
P
Pay Extra Attention While Using Public Wifi
Q
Quarantine All Unused Apps
R
Respect the Privacy of Others
S
Scan Any File Downloaded From Internet Before Opening/ Using/ Installing
T
Turn On Automatic Updates For Your Operating System
U
Use Strong Passwords With Personal Acronym
V
Verify With Whom You Are Interacting Online
W
Watch Out For Online Scams
X
Xtra Precaution For Your Online Financial Transactions
Y
Your Priority On Cyber Security Make You Cyber Aware Citizen
Z
Zero Participation in Dark Web
CyberSecurityNews.com
cybersecurity-news
The_Cyber_News


गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS
Indian
Cyber
Crime
Coordination
Centre
Indian Cybercrime Coordination Centre (I4C)
5th Floor, NDCC-II Building, Jai Singh Road,
New Delhi - India
By the mandate of Shri. Rajesh Kumar, CEO of the Indian Cyber Crime Coordination Centre; in partnership with Central Bureau of Investigation (CBI) which is the National Nodal Agency for INTERPOL in India; I hereby notify you of a computerized seizure of Cyber-infiltration captured on your internet protocol address (IP) in relation to the following analysis:-
**CHILD PORNOGRAPHY
**PEDOPHILIA
**CYBER PORNOGRAPHY
**EXHIBIT
**GROOMING
CERTIFIED COPY
The Criminal Code Of India Section 14 of the POCSO Act 2012, Section 292, Section 67A, and Section 67B of the Information Technology Act, of 2000 criminalizes the publication or transmission of sexually explicit acts or conduct in electronic form of Juvenile pornography and is punishable on first conviction by imprisonment.
The Central Bureau of Investigation (CBI) and Indian Cybercrime Units perform an investigative role against victims through the technology of information, suggests, Possess, produce, disseminate or access child pornographic images and materials within our territory.
The Government has also given a number of steps to be implemented by Internet Service Providers (ISPs) to protect children from sexual abuse online. These, inter-alia include:
Blocking of websites containing extreme Child sexual Abuse Material (CSAM) based on INTERPOL's "Worst-of-list" shared periodically by Central Bureau of Investigation (CBI) which is the National Nodal Agency for Interpol. The list is shared with Department of Telecommunications (DoT), who then directs major ISPs to block such websites.
For discretion sake, I decided to reach you privately before transferring your case files to the Justice prosecutors for immediate prosecution.
With immediate effect, respond to this message and state your justifications for a further review before appropriate sanctions will be impose within 24 hours.
Failure to respond within 24 hours from now, the prosecutor will establish an arrest warrant against you through the closest Police Station.
After prosecution, your information will be sent to the National Register for minor Sex Offenders, associations fighting against PEDOPHILIA and to the Media for publication.
Respond immediately.
Tapan Deka
Director of the Intelligence Bureau
Shri Rajesh Kumar
CEO, Indian Cyber Crime Coordination Centre
5th Floor, NDCC-II Building, Jai Singh Road, New Delhi - India
FRAUD ALERT
FRAUD ALERT
FRAUD ALERT
THIS INFORMATION IS
FAKE

CYBER LAWS-IT ACT

CYBER LAWS IN INDIA

IT ACT 2000

The information Technology Act is an outcome of the resolution dated 30th January 1997 of the General Assembly of the United Nations, which adopted the Model Law on Electronic Commerce, adopted the Model Law on Electronic Commerce on International Trade Law.

The Union Cabinet approved the bill on May 13, 2000 and on May 17, 2000, both the houses of the Indian Parliament passed the Information Technology Bill. The Bill received the assent of the President on 9th June 2000 and be known as the Information Technology Act, 2000. The Act came into force on 17th October 2000.

IT ACT AMENDMENT , 2008

IT Act was amended by Information Technology Amendment Bill, 2008 which was passed in Lok Sabha on 22nd December, 2008 and in Rajya Sabha on 23rd December, 2008. It received the assent of the President on 5th February 2009 and was notified with effect from 27/10/2009.

The IT Act, 2000 consists of 90 sections spread over 13 chapters [Sections 91, 92, 93 and 94 of the principal Act were omitted by the Information Technology (Amendment) Act 2008 and has 2 schedules.[Schedules III and IV were omitted by the Information Technology (Amendment) Act 2008].

COMPLIANCES
The Rules-I

- The Information Technology (Certifying Authorities) Rules 2000
- The Cyber Regulations Appellate Tribunal (Procedure) Rules 2000
- The IT (Certifying Authorities) Regulations 2001
- The IT(Other Powers of Civil Court vested in Cyber Appellate Tribunal) Rules 2003
- The IT(Other Standards) Rules 2003
- The IT (Qualification and Experience of Adjudicating Officers and Manner of Holding Enquiry) Rules 2003
- The IT (Use of Electronic Records and Digital Signature) Rules 2004
- The IT (Security Procedure) Rules 2004
- The Cyber Appellate Tribunal (Salary, Allowances and other terms and conditions of Service of Chairperson and Members) Rules 2009
- The Cyber Appellate Tribunal (Procedure for misbehavior or incapacity of Chairperson and Members) Rules 2009
- IT (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009
- IT (Procedure and Safeguards for Blocking for Access of Information by Public) Rules 2009

The Rules-II

- IT (Procedure and Safeguards for Monitoring and Collecting Traffic Data or Information) Rules 2009
- IT (T (Guidelines for Cyber Café) Rules 2011
- IT (Electronic Service Delivery) Rules 2011
- The Information Technology Reasonable Security Practices And Procedures And Sensitive Personal Data or Information)Rules, 2011)
- IT (National Critical Information Infrastructure Protection Centre and Manner of Performing Functions and Duties) Rules 2013
- IT (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules 2013
- The Digital Signature (End Entity) Rules 2015
- CERT-IN Rules 2022
- The Information Technology (Intermediary Guidelines And Digital Media Ethics Code) Rules, 2021/2022/2023

PRIVACY ISSUES IN CYBER SPACE

Traditionally privacy was the concern against 'state' interference only (or at least to a great extent)

•However with the growth of digital age –more and more information finds its way into massive databases held predominantly by private players along with governments

HOW PI IS USED OR SHARED

HOW PI IS PROTECTED

WHO WOULD BE ACCOUNTABLE FOR ITS MISUSE

IT ACT 2000

IT ACT AMENDMENT 2008

Right to Privacy as a Fundamental Right

Data Privacy and Breach Disclosure Dilemmas

APPLICABILITY OF DATA PROTECTION LAWS

FINES IMPOSED

DATA PROTECTION AUTORITHY ACTIVITY

Total amount of GDPR fines by country

ITALY	€ 70.290.601
GERMANY	€ 63.386.633
FRANCE	€ 54.436.300
UNITED KINGDOM	€ 44.221.000
SPAIN	€ 15.608.410
SWEDEN	€ 14.332.430
THE NETHERLANDS	€ 3.490.000
BULGARIA	€ 3.210.690
NORWAY	€ 1.257.150
POLAND	€ 1.741.948
BELGIUM	€ 872.000
GREECE	€ 765.000
ROMANIA	€ 669.150
HUNGARY	€ 633.011
IRELAND	€ 630.000
DENMARK	€ 563.150
PORTUGAL	€ 424.000
ESTONIA	€ 300.548
FINLAND	€ 207.500
LATVIA	€ 178.250
CYPRUS	€ 143.000
CZECH REPUBLIC	€ 137.866
SLOVAKIA	€ 90.000
LITHUANIA	€ 76.500
AUSTRIA	€ 70.950
ICELAND	€ 29.600
ISLE OF MAN	€ 13.500
MALTA	€ 5.000
CROATIA	UNKNOWN

TOP 5 BIGGEST GDPR FINES

1	Google Inc.		€50 000 000
2	H&M Hennes & Mauritz		€35 258 708
3	TIM - Telecom Provider		€27 800 000
4	British Airways		€22 046 000
5	Marriott International		€20 450 000

CERT-IN-28-4-2022

Applicability: 60 Days from issue date, so effectively applicable from 28 June 2022 – by all service providers, intermediaries, data centers, corporate bodies, & govt organizations.
Non-Compliance: Failure to follow these directions may result in the penalty as per sub-section (7) of section 70B of the IT Act, 2000 and other laws as applicable: "Punishable up to a year in imprisonment or with a fine of up to one lakh rupees or both."

Designate a Point of Contact to interface with CERT-In

The Point of Contact details shall be sent to CERT-In via email (info@cert-in.org.in) in the format specified in Annexure II of the directions document.

Types of Cyber Security Incidents to be reported

The details are specified in Annexure II of the directions document, along with a reference to Rule 12(1)(a) of the IT Rules 2013.

Incident Reporting

Mandatorily report cyber incidents within 6 hours of noticing such incidents or being brought to notice about such incidents. The incidents can be reported to CERT-In via email (incident@cert-in.org.in), phone (1800-11-4949), or fax (1800-11-6969). Template and other details of reporting are available at:

- https://www.cert-in.org.in/SecurityIncident.jsp

Cyber Security Mitigation Actions when required by CERT-In

Entity must provide information and/or assistance to CERT-In as may be required for incident response, mitigation, and on an as-required basis for enhanced cybersecurity awareness.

Synchronization of Information & Communications Technology (ICT) Systems Clocks

Connect to the Network Time Protocol (NTP) Server of the National Informatics Centre (NIC) or National Physical Laboratory (NPL), or with NTP servers traceable to these NTP servers.

Log Retention and Management

Enable logs of all the ICT systems and maintain securely for a rolling period of 180 days within Indian jurisdiction; and be provided to CERT-In on an as-needed basis.

Register subscriber/customer information

- Applicability: Data Centers, Virtual Private Server (VPS) providers, Cloud Service providers, and Virtual Private Network (VPN) providers.
- Register user, IP, and other information; and maintain them for 5 years or longer as mandated by the law after any cancellation or withdrawal of the registration.

KYC Requirements

- Applicability: Virtual asset service providers, virtual asset exchange providers, and custodian wallet providers.
- Maintain all information obtained as part of Know Your Customer (KYC) and records of financial transactions for 5 years to ensure cybersecurity in the payments industry and the protection of citizen data.

- DATA BREACH INSURANCE
- In order to mitigate the risk that comes along with data loss, many companies are now purchasing data breach insurance.
- Data breach insurance helps cover the costs associated with a data security breach. It can be used to support and protect a wide range of components, such as public relations crises, protection solutions and liability. It may also cover any legal fees accumulated from the breach.

I T - LAWS

INFORMATION TECHNOLOGY ACT, 2000 (ITAA 2008)

- Source
- The **General Assembly of the United Nations** by resolution A/RES/51/162,dated 30th January, 1997 has adopted the **Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law**;
- In India our Parliament gave effect to this resolution of the General Assembly of the United Nations for adoption of a Modern Law on Electronic Commerce. The consequence was the passing of Information Technology Act 2000.

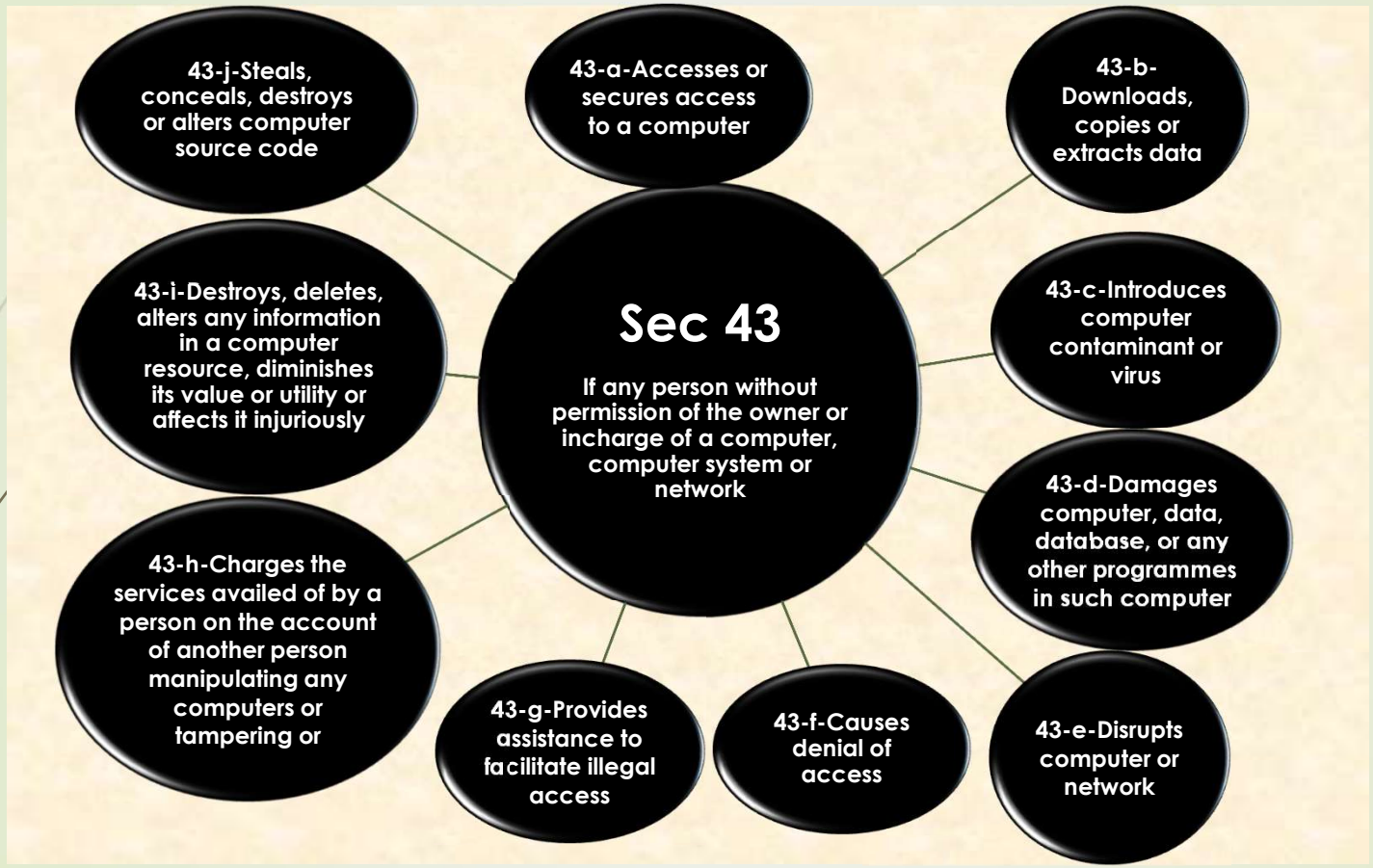
Aim, Objectives of I T Act,2000

- The Act essentially deals with the following issues:
  - Legal Recognition of Electronic Documents
  - Legal Recognition of Digital Signatures (Asymmetric Crypto System for the creation and verification of Digital signature in India)
  - To provide mechanism for regulation of Electronic Commerce.
  - To facilitate e-filing of documents with the government agencies
  - Offences and Contraventions
  - Justice Dispensation Systems for cyber crimes.

AMENDMENT OF IT ACT

- **Information Technology Amendment Act 2008** was placed in the Parliament and passed at the end of 2008. 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
  - Authorizing an Inspector to investigate cyber offenses


Sec 43
If any person without permission of the owner or incharge of a computer, computer system or network
43-a-Accesses or secures access to a computer
43-b-Downloads, copies or extracts data
43-c-Introduces computer contaminant or virus
43-d-Damages computer, data, database, or any other programmes in such computer
43-e-Disrupts computer or network
43-f-Causes denial of access
43-g-Provides assistance to facilitate illegal access
43-h-Charges the services availed of by a person on the account of another person manipulating any computers or tampering or
43-i-Destroys, deletes, alters any information in a computer resource, diminishes its value or utility or affects it injuriously
43-j-Steals, conceals, destroys or alters computer source code

Section 43A. **Compensation for failure to protect data. -** Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource 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, such body corporate shall be liable to pay damages by way of compensation, to the person so affected.

Explanation: For the purposes of this section
(i) "body corporate" means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities
(ii) "reasonable security practices and procedures" means security practices and procedures designed to protect such information from unauthorised access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.
(iii) "sensitive personal data or information" means such personal information as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.

-The Information Technology Reasonable Security Practices And Procedures And Sensitive Personal Data or Information)Rules, 2011)

-Judgements-IT Secretary-SIM SWAP CASE

-NOW DPDP-2023

- The Information Technology Reasonable Security Practices And Procedures And Sensitive Personal Data or Information)Rules, 2011)

- Necessitates that every body corporate SHALL
  - lay down strict privacy policy
  - Follows stringent procedures as laid down in The Rule 2011 for collection of information
  - Be vigilant and cautious in disclosure of information
  - Be vigilant and cautious in transfer of information
  - Adhere to reasonable security practices and procedures

Indian Data Protection Regime Evolution

2008	IT (Amendment) Act Privacy clauses
2011	Notification of privacy rules under Sec 43A of IT Amendment Act 2008
2012	Framework by A P Shah Expert Group on Privacy; DoPT draft law
2014	Security-Privacy Framework for Smart Cities
2015	RBI Cyber Security Framework; SEBI Cyber Security Guidelines
2016	Aadhaar Law and Regulations focusing on Privacy; IRDAI Cyber Security Framework
2017	Supreme Court declares 'Right to Privacy' as Fundamental; Govt. creates a Committee and opens up consultation on drafting a new data protection law
2018	Draft Data Protection Bill & Report by Srikishna Committee; Aadhaar Supreme Court Judgment; Draft Healthcare Act (Disha)
2019	Updated Draft Data Protection Bill Tabled in Parliament; Parliamentary Committee convened Withdrawn-2022
2022	Digital Personal Data ProtectionAct , 2023

CYBER-IT ACT OFFENCES

Sec 65	• Tampering with Computer Source Documents
Sec 66	• Computer related offences
Sec 66 B	• Dishonestly receiving stolen computer resource or communication device

Sec 66 C	• **Punishment for Identity Theft**
Sec 66 D	• **Cheating by Personation by using Computer Resource 7 Communication Device**
Sec 66 E	• **Violation of Body Privacy**
Sec 66 F	• **Cyber Terrorism**

Sec 67

- **Publishing or transmitting Obscene material in Electronic form(Obscenity)**

Sec 67 A

- **Publishing or transmitting of material containing Sexually Explicit Act, etc. in electronic form (Porn Content)**

Sec 67 B

- **Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form(Child Porn)**
- **Also-Obscene and Indecent**

Sec.67C	• **Preservation and Retention of information by intermediaries**
Sec.69	• **Powers to issue directions for interception or monitoring or decryption of any information through any computer resource**
Sec 69A	• **Power to issue directions for blocking for public access of any information through any computer resource**
Sec 69 B	• **Power to authorize to monitor and collect traffic data or information through any computer resource for Cyber Security**

Sec 70	• **Un-authorized access to protected system**
Sec 71	• **Penalty for misrepresentation**
Sec 72	• **Breach of confidentiality and privacy**
Sec 72A	• **Punishment for Disclosure of information in breach of lawful contract**
Sec 73	• **Publishing False digital signature certificates**

Sec 74	• **Publication for fraudulent purpose**
Sec 75	• **Act to apply for offence or contraventions committed outside India**
SEC 77 A	• **Compounding of Offences**
Sec 77 B	• **Offences with three years imprisonment to be cognizable**
Sec 79	• **Exemption from liability of intermediary in certain cases** • Intermediary Rules and **Now Rules 2021/2022**

Sec 79 A	• Examiner of Electronic Evidence
Sec 84 B	• Punishment for abetment of offences
Sec 84 C	• Punishment for attempt to commit offences
Sec 85	• Offences by Companies

CYBER SECURITY

- **DESKTOP/LAPTOP AND PRINTER SECURITY AT OFFICE**

1. Use only Standard User (non-administrator) account for accessing the computer/laptops for regular work. Admin access to be given to users with approval of CISO only.
2. Set BIOS Password for booting.
3. Ensure that the Operating System and BIOS firmware are updated with the latest updates/patches.
4. Set Operating System updates to auto-updated from a trusted source.
5. Ensure that the Antivirus client installed on your systems are updated with the latest virus definitions, signatures and patches.
6. Only Applications/software's, which are part of the allowed list authorized by CISO, shall be used; any application/software which is not part of the authorized list approved by CISO, shall not be used.
7. Always lock/log off from the desktop when not in use.
8. Shutdown the desktop before leaving the office.

1. Keep printer's software updated with the latest updates/patches.
2. Setup unique pass codes for shared printers.
3. Internet access to the printer should not be allowed.
4. Printer to be configured to disallow storing of print history.
5. Enable Desktop Firewall for controlling information access.
6. Keep the GPS, Bluetooth, NFC and other sensors disabled on the desktops /laptops and mobile phones. They may be enabled only when required.
7. Use a Hardware VPN Token for connecting to any IT Assets located in Data Centre.
8. Do not write passwords, IP addresses, network diagrams or other sensitive information on any unsecured material (ex: sticky/post-it notes, plain paper pinned or posted on users table etc.).
9. Do not use any external mobile App based scanner services (ex: **Cam scanner**) for scanning internal government documents.
10. Use of all pirated Operating systems and other software/applications that are not part of the authorized list of software's should be immediately deleted

- **PASSWORD MANAGEMENT**

1. Use complex passwords with a minimum length of 8 characters, using a combination of capital letters, small letters, numbers and special characters.
2. Change passwords at least once in 30 days.
3. Use Multi-Factor Authentication, wherever available.
4. Don't use the same password in multiple services/websites/apps.
5. Don't save passwords in the browser or in any unprotected documents.
6. Don't write down any passwords, IP addresses, network diagrams or other sensitive information on any unsecured material (ex: sticky/post-it notes, plain paper pinned or posted on your table).
7. Don't share system passwords or printer pass code or Wi-Fi passwords with any unauthorized persons.

- **INTERNET BROWSING SECURITY**

1. While accessing Government applications/services, email services or banking/payment related services or any other important application/services, always use Private Browsing/Incognito Mode in your browser.
2. While accessing sites where user login is required, always type the site's domain name/URL, manually on the browser's address bar, rather than clicking on any link.
3. Use the latest version of the internet browser and ensure that the browser is updated with the latest updates/patches.
4. Don't store any usernames and passwords on the internet browser.
5. Don't store any payment related information on the internet browser.
6. Don't use any 3rd party anonymization services (ex: Nord VPN, Express VPN, Tor, Proxies etc).
7. Don't use any 3rd party toolbars (ex: download manager, weather tool bar, ask me tool bar etc.) in your internet browser.
8. Don't download any unauthorized or pirated content /software from the internet (ex: pirated - movies, songs, e-books, software's).
9. Don't use your official systems for installing or playing any Games.
10. Observe caution while opening any shortened URLs (ex: tinyurl.com/ab534/). Many malwares and phishing sites abuse URL shortener services. Such links may lead to a phishing/malware webpage, which could compromise your device

- **MOBILE SECURITY**

1. Ensure that the mobile operating system is updated with the latest available updates/patches.
2. Don't root or jailbreak your mobile device. Rooting or Jail breaking process disables many in-built security protections and could leave your device vulnerable to security threats.
3. Keep the Wi-Fi, GPS, Bluetooth, NFC and other sensors disabled on the mobile phones. They may be enabled only when required.
4. Download Apps from official app stores of Google (for android) and apple (for iOS).
5. Before downloading an App, check the popularity of the app and read the user reviews.
6. Observe caution before downloading any apps which has a bad reputation or less user base etc.
7. While participating in any sensitive discussions, switch-off the mobile phone or leave the mobile in a secured area outside the discussion room.
8. Don't accept any unknown request for Bluetooth pairing or file sharing.

1. Before installing an App, to carefully read and understand the device permissions required by the App along with the purpose of each permission.
2. In case of any disparity between the permissions requested and the functionality provided by an app, users to be advised not to install the App (Ex: A calculator app requesting GPS and Bluetooth permission).
3. Note down the unique 15-digit IMEI number of the mobile device and keep it offline. It can be useful for reporting in case of physical loss of mobile device.
4. Use auto lock to automatically lock the phone or keypad lock protected by pass code/ security patterns to restrict access to your mobile phone.
5. Use the feature of Mobile Tracking which automatically sends messages to two preselected phone numbers of your choice which could help if the mobile phone is lost/ stolen.
6. Take regular offline backup of your phone and external/internal memory card.
7. Before transferring the data to Mobile from computer, the data should be scanned with Antivirus having the latest updates.
8. Observe caution while opening any links shared through SMS or social media etc., where the links are preceded by exciting offers/discounts etc., or may claim to provide details about any latest news. Such links may lead to a phishing/malware webpage, which could compromise your device.
9. Report lost or stolen devices immediately to the nearest Police Station and concerned service provider.
10. Disable automatic downloads in your phone.
11. Always keep an updated antivirus security solution installed

- **EMAIL SECURITY**

1. Ensure that Kavach Multi-Factor Authentication is configured on the NIC Email Account.
2. Download kavach app from valid mobile app stores only. Do not download from any website.
3. Do not share the email password or Kavach OTP with any unauthorized persons.
4. Don't use any unauthorized/external email services for official communication.
5. Don't click/open any link or attachment contained in mails sent by unknown sender.
6. Regularly review the past login activities on NIC's Email service by clicking on the "login history" tab. If any discrepancy is observed in the login history, then the same should be immediately reported to NIC-CERT.
7. Use PGP or digital certificate to encrypt e-mails that contains important information.
8. Observe caution with documents containing macros while downloading attachments, always select the "disable macros" option and ensure that protected mode is enabled on your office productivity applications like MS Office.

- **REMOVABLE MEDIA SECURITY**

1. Perform a low format of the removable media before the firsttime usage.
2. Perform a secure wipe to delete the contents of the removable media.
3. Scan the removable media with Antivirus software before accessing it.
4. Encrypt the files /folders on the removable media.
5. Always protect your documents with strong password.
6. Don’t plug-in the removable media on any unauthorized devices

- **SOCIAL MEDIA SECURITY**

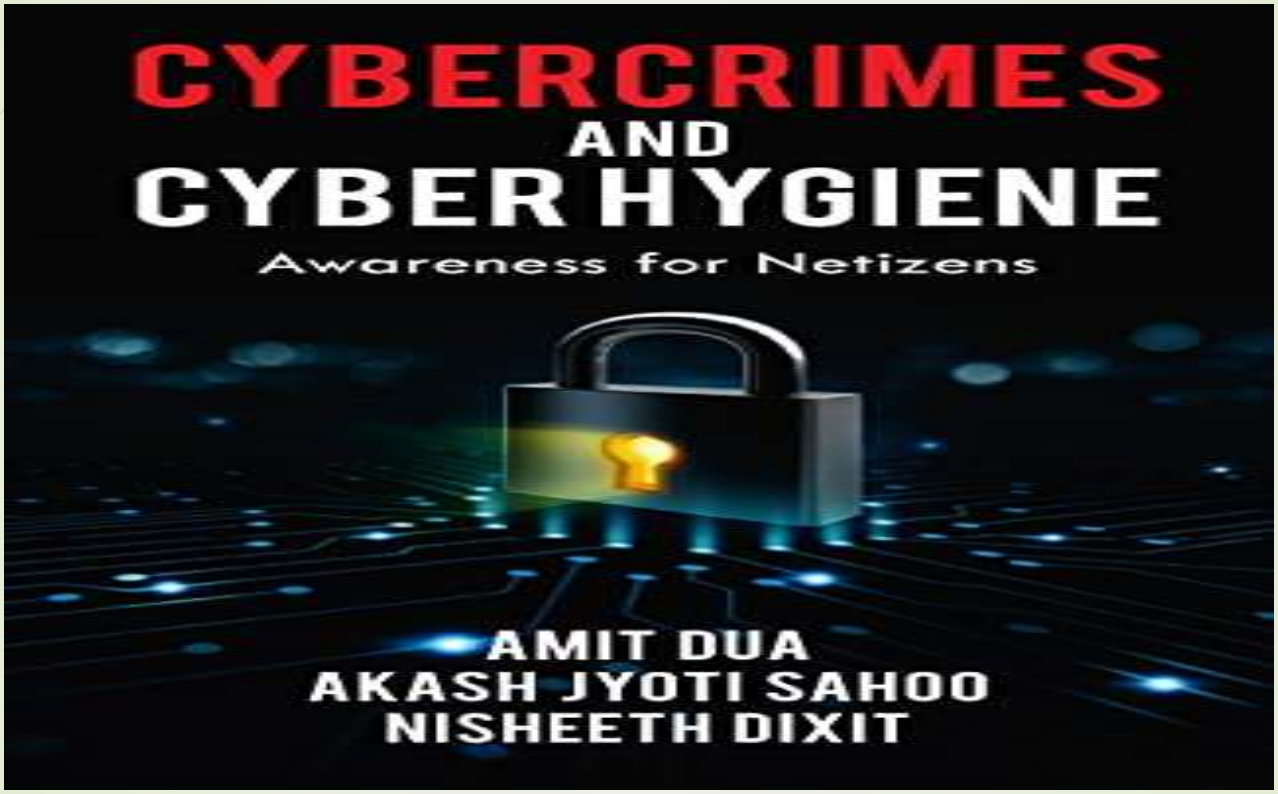
1. Limit and control the use/exposure of personal information while accessing social media and networking sites.
2. Always check the authenticity of the person before accepting a request as friend/contact.
3. Use Multi-Factor authentication to secure the social media accounts.
4. Do not click on the links or files sent by any unknown contact/user.
5. Do not publish or post or share any internal government documents or information on social media.
6. Do not publish or post or share any unverified information through social media.
7. Do not give share the @gov.in/@nic.in email address on any social media platform.
8. It is recommended to use NIC's Sandes App instead of any 3rd party messaging app, for official communication

- SECURITY ADVISORY AND INCIDENT REPORTING
  Adhere to the Security Advisories published by NIC-CERT (https://niccert.nic.in) and CERT-In (https://www.cert-in.org.in).

- Report any cyber security incident, including suspicious mails and phishing mails to NIC-CERT (incident@nic-cert.nic.in) and CERT-In (incident@cert.org.in).

ND CYBERLAW

ZERO TRUST


CYBERCRIMES
AND
CYBER HYGIENE
Awareness for Netizens
AMIT DUA
AKASH JYOTI SAHOO
NISHEETH DIXIT

THANKS

NISHEETH DIXIT

ADVOCATE

9829112511

www.ndcyberlaw.com

- *The contents / images /vidoes/ photographs are used only for information and education purposes only*