Handbook on Basics of Digital Hygiene for Higher Education Institutions

CHAPTERS

1. Introduction

- A shift towards virtual classroom and collaborative learning environment
- Newer technologies being used to conduct virtual classrooms
- Redefined objectives of a teacher for conducting virtual classes
- Redefined behavior protocols for a student in virtual classes
- Need and purpose for such a handbook and guidelines on how to use it

2. ***Basic Concepts and Definitions*** to explain basic concepts such as

- Digitalization
- Common terms - Cyberspace, digital footprints, digital profiling, hacking, data breach, deep/dark web
- Threat Landscape: Victim, Actor, Motive, Vectors, Techniques
- Why do people fall victim to cybercrimes?
- Information Security - CIA Triad, RMIAS Model

3. ***Trending Cybercrimes***[1]

a. Phishing

- Email, Fake Messages, SMS, Call based Phishing
    - Spear Phishing / Whaling
    - fraud calls /videos Vishing
    - fake websites

b. Online Financial frauds

- Internet banking-related fraudUPI fraud
- OTP Frauds (Mentioned separately as its Modus Operandi differs from UPI Frauds)
- e-Wallet frauds
- Debit/Credit Card/ Sim swap/ Sim cloning fraud
- Demat/depository fraud

c. Cryptocurrency fraudSocial Media Crimes

- Cyberstalking
- Cyberbullying
- Sexting
- Honey Trapping
- Trolling
- Morphing
- Grooming

d. Mobile Apps – Websites-based issue.

[1] *(*** with related Case Studies (with special emphasis on case-stories related to teaching/learning environment and preferably anonymised or attributed / illustrations (preferably pick up from CyberDost)*

- Dangerous game challenges
- Malicious Apps
- Matrimonial/ career frauds
- Malware and Types
- Virus
- Worm
- Trojan
- Backdoor, RootKit, Botnets
- Damage to computer systems
- Unauthorized access
- Data breach
- Some other cybercrime and related instances
- Spoofing
- IoT Attacks
- Advanced persistent threats
- Scareware
- Adware

4. A Ready Reckoner to Stay CyberSafe

- Secure E-Commerce Usage: (Do not blindly go on reviews, Genuine Websites, etc.)
  Secure Computer/Laptop Usage: Strong Password, Updated Antivirus, and Systems, Refrain Admin Accounts, etc.
- Secure Mobile Phone Practices: Password/Pattern, Find My Device, Disk Encryption, Location-Privacy settings, Unknown – Third-Party App Risks, etc.
  - Secure Internet Usage (Antivirus, Pop-up protection, File Download, etc.)
  - How to Use Digilocker to keep originals.
  - Preventive measure
  - Tools to Safeguard

5. Demystifying Institutional framework of Cyber Security in India

- NCSC
- MeitY – CERT-In- Cyber Swachhta Kendra (Botnet cleaning and Malware Analysis Centre), ISEA, Cyber Surakshit Bharat Programme
- NCIIPC
  - National Cyber Coordination Centre (NCCC)
  - MHA – CIS Division, Indian Cybercrime Coordination Center (CyberDost and its Handles)
  - State Cyber Cells (Police is a State Subject)
  - CDAC

6. Glimpses into Legal framework for Cyber Security and Privacy in India

- IT Act, 2000 / ITAA 2008

- IPC, 1860
- National Cyber Security Policy, 2013

7. What to Do if Victim of a Cybercrime

(i) How and Where to Lodge a Cyber Crime Complaint [2]

  (i) Helplines and Portals. (Women and Children)

8. Strengthening Students

(ii) Career Opportunities (Job Profiles, Universities, and related certifications)

(iii) MOOC (NCTC)

9 Strengthening Educational Setups

- Tool Kits available –CCMP and other related sources available
- Suggested Cyber Policy Guidelines for HEIs
- NISPG Guidelines by MHA

10. Strengthening Teachers & IT Teams of HEIs

- Some Existing Training Initiatives (including CISO training)
- Reference Resources for Teachers / IT teams of Educational Institutes[3]

11. Bibliography/ References

***12.* Glossary of Terms / Abbreviations Used**

[2] maybe we give a simple template for lodging a cyber-complaint

[3] *(May be later create a Trainer Manual for them, Conduct ToTs for them)*

Handbook on Basics of Digital Hygiene for Higher Education Institutions

INTRODUCTION

In the emerging era of digitalization, education requires tech-assisted teaching, learning solutions, and fast-paced innovations. Students and teachers now have access to smart mobile devices as well as a variety of remote e-learning and evaluation options. The various e-learning tools like smartboards, projectors have been promoted in educational institutions for better understanding and learning.

A shift towards Virtual Classrooms and Collaborative Learning Environment

Traditional classroom and distant learning experiences have been greatly enhanced by digital tools and techniques. Whiteboards and smartboards, for example, are excellent tools for visually explaining concepts and making the teaching-learning process truly interactive. The smartboards have touch screen displays that allow the user to move objects around on the board with their fingers and write on them using tools which is possible on traditional blackboards.

The virtual classroom essentially duplicates the physical classroom environment, but without the constraints of time and location. It also saves the expenses of putting up physical classrooms in different places, and provides the ability for professors and students to teach and learn almost anywhere and at any time, as well as the ability to record the lectures and share it later.

The convenience of online courses and certifications, as well as the availability of large digital resources with micro-learning modules, have made them increasingly popular among students and educators worldwide as this model provides learners with various options at ease.

Newer Technologies being used to Conduct Virtual Classrooms

According to the Pearson Global Learner Survey, 78 percent of Indian students say that technology aids their learning and makes it fun. Artificial Intelligence (AI) and Machine Learning (ML) technologies, for example, can help personalize learning processes for each student depending on their ability, preferred learning mode, and experience. Instead of providing a single curriculum for all students, educators will be aided by AI, which will use the same basic curriculum to give a wide range of hyper-personalized information tailored to each student's individual needs.

Apart from AI, augmented reality (AR) and virtual reality (VR) are projected to become more popular in classrooms and experiments. Many tech companies are now focusing on the education industry, with purpose-built hardware, platforms, and digital tools aimed at elevating the classroom learning experience.

Redefined Objectives of a Teacher for conducting Virtual Classes

Virtual classrooms have brought a distinct perspective on the teaching-learning process as we move to teach online. A professor conducts the discussions in an online setting, but differently, as a facilitator. Student learning is more about their ability to grasp knowledge than it is about the professor.

Technology plays a role in e-learning, and online teaching necessitates some technological knowledge. However, the technical components of running an online course are more complex than they appear. The online educator takes on the role of tech specialist, selecting tools that are suitable for learning objectives and within students' technical skills.

It is futile to simply replicate the course in an online format by uploading lectures and handouts. As the delivery media are diverse, different approaches are necessary. The online educator takes on the role of e-learning designer, rethinking and redesigning the course for the online space.

To bring the virtual classroom to life, the educator must actively build a sense of connectedness and introduce forms of communication among all students using online live cameras, emails, discussion forums, chat rooms, multimedia, or other methods. Personal introductions, chat rooms, prompt responses to inquiries, and prompt feedback on tasks are all examples of how this might be accomplished.

Redefined Behavior Protocols for a Student in Virtual Classes

There are numerous crucial characteristics of remote teaching that might be detrimental to the entire school community. Teachers, on the other hand, should be concerned about attacks that occur during virtual classroom lectures while the discussion is in progress. These threats can be divided into two categories:

1) the violation of the classroom as a safe and secure learning environment, and

2) the invasion of the privacy of the school community which includes students too.

Risk can be reduced in online classes by taking the following basic precautions:

- Join the online classroom by using URLs shared only by authorized and confirmed faculty IDs.
- Faculty should always make the classroom URL unique and/or secure access with a strong password.
- Faculty should enable waiting room feature.The educator can establish norms and protocols for online classes.
- Do not publish the virtual session URL or classroom information on any public forum including WhatsApp groups.
- Do not reveal any personal information until it is verified that everyone in the virtual session has permission to be there.
- Always be aware of what has been presented in the classroom, and prohibit the things which disobey/break the guidelines right away.

CHAPTER 2

BASIC CONCEPTS AND DEFINITIONS

DIGITALIZATION AND ITS BENEFITS

Digitalization is the process of using new IT technologies to maximize the use of the digital resources available. The use of digital technologies to modify a business model and generate new revenue and value-producing opportunities is known as digitalization; it is the transition to a digital business.

Digitalization

Due to the centralization and accessibility of data, the digital era delivers all types of information at our disposal.

Nowadays, countless apps allow users to send messages instantly. Digitalization has also transformed the ability of the user to communicate. For example, in a social media post, saying someone's name or making a video. It has also given a better platform to users to share new ideas and to spread them more efficiently.

Digitalization has opened up a new universe of career opportunities for information technology professionals where the Internet has provided the facility to the user to work from remote areas where the employee is not required to be present physically.

Moreover, digitalization has boosted up commercial competition to the point where customers now have a greater variety of choices*. Digital currency is another benefit of the digital era, as it speeds up and simplifies financial transactions.

CYBERSPACE

According to the National Institute of Standards and Technology, cyberspace is “A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.” In simple words, cyberspace is a virtual environment of interconnected network and digital systems to facilitate communication among various objects present in that network.

DIGITAL FOOTPRINTS

It is abundantly clear that we live in the Big Data world where “Right to be Forgotten” or “Right to be Erased” is not that easy as the identity of an individual is disclosed not only privately but on public platforms too. The metadata plays an important role due to which digital footprints are always left behind in one form or another to find the digital trail towards an individual. Your likes on social media posts, the content that you watch, web cookies on the websites you visit, etc., can make up your digital footprints.

DEEP WEB

The deep web is a part of the internet that isn't indexed by the standard search engines. The deep web is located under the surface and contains around 90% of all web pages.Visiting this part of the web would not pose any threat to your computer or your data.

The following are some of the largest parts of the deep web:

- **Databases** are file collections, both public and private, that are not connected to other parts of the web and may only be searched within the database itself.
- **Intranets** are private networks used by businesses, governments, and educational institutions to communicate and regulate aspects of their operations.

DARK WEB

The dark web is a subset of the deep web that is intentionally hidden, requiring a specific browser—Tor—to access.

The dark web is a part of the deep web but only covers a small part of it. The dark web is a hidden collective of websites that can only be accessed with a specialized web browser. It's used to keep internet activity private and anonymous, which can be useful in both legal and unlawful situations.

These are mostly onion sites that can be accessed via Tor and their domain names are made in a manner so that they are hard to remember. The dark web's reputation has been associated with criminal intent or illegal activities, as well as "trading" sites where users can buy illegal items or services. Legal parties, on the other hand, have taken advantage of this framework as well. [4]**Why Do People Fall Victim to Cyber Crimes?**

Biggest myth is that I will never be hacked. It is a prevalent cyber pronoun – “There are two kinds of people. One who has been hacked and the other who will soon be hacked.”

People fall prey to cybercrimes, majorly, for the following reasons:

➔ Trusting strangers - Scammers' strategies have considerably advanced and appear genuine to the innocent victims. Hackers have recently started breaking into company networks and sending emails posing as coworkers, asking for sensitive information such as passwords and company credit card details.

➔ Unawareness – Being unaware of the current trends in cybercrimes can cause a person to become a victim of one. Cyber attackers spend months analyzing their target and searching for loopholes. These perpetrators create a sense of urgency and take advantage of the confusion on the part of the victim to deceive them into giving their sensitive financial /personal information.

➔ Underestimating the risk - Victims usually underestimate the risk of cybercrimes. It's all too easy to get complacent over time, putting oneself at risk of becoming a target.

THREAT LANDSCAPES

[4] Available at https://www.kaspersky.com/resource-center/threats/deep-web as accessed on 11-02-2022

TARGETS

Target/victim could be an individual, organization, or nation.

THREAT ACTORS

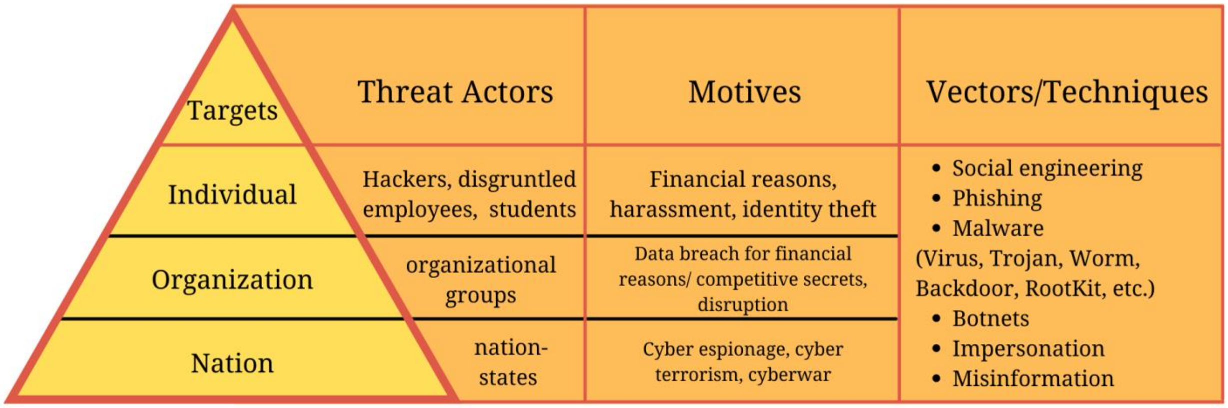
The threat actors include cybercriminals, malicious insiders, or hacker groups which are a threat to the IT Security of any individual, organization, or nation who hacked their data or made their data inaccessible for malicious reasons.

MOTIVES/REASONS

Threat actors' motives can be anything from amusement to financial gains. The different cyberattacks vary from an individual, organization, or nation by way of disruption of various services which affects their financial capacity through misleading, deceptive or illegal practices or cyber espionage which is a kind of cyberattack by accessing the sensitive data for economic gains. These will be further explained in this chapter later.

ATTACK VECTORS

Attack vector in cybersecurity is a kind of method that a hacker uses to breache the security or to infiltrate the users' network. Attack vector includes viruses like malware, Ransomware, Trojan, etc or other cybercrime techniques.



Targets	Threat Actors	Motives	Vectors/Techniques
Individual	Hackers, disgruntled employees, students	Financial reasons, harassment, identity theft	• Social engineering • Phishing • Malware (Virus, Trojan, Worm, Backdoor, RootKit, etc.) • Botnets • Impersonation • Misinformation
Organization	organizational groups	Data breach for financial reasons/ competitive secrets, disruption	
Nation	nation-states	Cyber espionage, cyber terrorism, cyberwar	

COMMON CYBERCRIME TECHNIQUES

Social Engineering

Social engineering assaults usually include psychological manipulation to persuade unaware users. It involves calling, sending an email or other message to a target that elicits feelings of urgency, fear, or other comparable emotions, prompting the victim to reveal sensitive information, click a harmful link, or open a malicious file. People often find it difficult to avoid such attacks. Some of the most common social engineering tactics are phishing via SMS or email, baiting individuals by offering free giveaways or by using scareware. All these methods will be later explained in detail. The Kali Linux operating system also offers some social engineering attack tools for free like Maltego and Social Engineering Toolkit(SET), etc.

Misinformation/Disinformation

Misinformation is simply false information that is disseminated, whether or not the purpose is to deceive, whereas disinformation is intentionally misleading or biased information that is based on distorted narratives or facts to achieve propaganda.

Standards on Disinformation and Propaganda:

a. General prohibitions on the dissemination of information based on vague and ambiguous ideas, including “false news” or “non-objective information”, are incompatible with international standards for restrictions on freedom of expression, as set out in paragraph 1(a), and should be abolished.

b. Criminal defamation laws are unduly restrictive and should be abolished. Civil law rules on liability for false and defamatory statements are legitimate only if defendants are given a full opportunity and fail to prove the truth of those statements and also benefit from other defences, such as fair comment.

c. State actors should not make, sponsor, encourage or further disseminate statements which they know or reasonably should know to be false (disinformation) or which demonstrate a reckless disregard for verifiable information (propaganda).

d. State actors should, in accordance with their domestic and international legal obligations and their public duties, take care to ensure that they disseminate reliable and trustworthy information, including about matters of public interest, such as the economy, public health, security and the environment[5]

Deep Fakes

Deep Fakes are a new and complex type of audio, video, or image creation technology that uses a form artificial intelligence called deep learning and is typically used for malicious purposes. They can quickly spread fraudulent words and actions to a global audience, and they can be difficult to tell apart from genuine information.

Case: In early 2020, a bank manager in the Hong Kong received a call from a man whose voice he recognized as the director of a company with whom he had spoken to and worked with before. He told the bank manager that his company was about to make an acquisition and so he needed the bank to authorize some transfers of around $35 million. Believing everything was legitimate, the manager authorized and initiated the transfer. What he didn’t know was the transfer was going straight into the accounts of the criminals.[6]

Impersonation

Impersonation is used as a technique where basic credentials are stolen. The threat actor or bad actor pretends to be someone else by adopting that person's identity to get access to resources, credit, or other benefits in that person's name and fame.

Spoofing

Spoofing occurs when cyber threat actors try to hide their true identities by faking the sender of a message to regularly fool the recipient by thinking that it came from someone else. To illicitly take information from a receiver, harvest user login credentials, perpetrate fraud, or spread malware, cyber threat actors frequently fake electronic communications from the targeted organization or a trusted partner.

[5] Available at https://www.osce.org/files/f/documents/6/8/302796.pdf

[6] Available at https://www.forbes.com/sites/thomasbrewster/2021/10/14/huge-bank-fraud-uses-deep-fake-voice-tech-to-steal-millions/?sh=462e58e47559 as accessed on 11-02-2022.

Example: Spoofing of Caller ID and Phone Numbers - forges the phone number or caller ID shown on incoming calls and text messages.

Morphing

Morphing is the process of smoothly transitioning from one image to another without any changes using online morphing tools. Usually, girls are harmed by this sort of morphing, which involves downloading photographs of girls from numerous social media sites using fake or real profiles and then morphing them. By threatening to publish the morphed photographs, these transformed images might be used to blackmail the girl or her family. Now-a-days, deep fake technology is also being used to morph the images and create fake videos of victims to deceive/harass their families.

Man-In-The-Middle

Man-in-the-Middle (MITM) attacks occur when an attacker intercepts communications between two parties. These attacks allow attackers to intrude and eavesdrop on the communication or data transfer between the two targets, as well as change the traffic flowing between them. The ‘targets' in these attacks are usually a human and a service. The attacker can take a passive role in the chat or go as far as stealing credentials, altering emails and other messages, or impersonating the person being talked to.

MOTIVES/REASONS FOR CYBERATTACKS

Identity/Credential Theft

Identity theft is the obtaining of some other person's personal information without their permission. Personal information may contain a person's name, phone number, address, bank account number, Aadhaar number, credit/debit card number, passwords among other things. Identity theft includes the theft of personal information that allows cyber thieves to impersonate another individual. Identity Theft takes place through access to social media accounts, personal documents, or skimming of credit/debit cards. The identity theft can be carried out by using sophisticated cyberattack techniques like social engineering, phishing attack and malwares. According to Norton Cyber Safety Insights report, almost percent of adult internet users in India faced identity theft in one way or the other in the year 2020 alone making it the biggest cyber security threat in India.[7]

Identity Fraud

Identity frauds happens when someone uses the stolen identity to commit fraud of various kinds. A person's identity and personal information are wrongfully used to gain access to various resources, services or goods. Examples of such fraud include opening a bank account, obtaining credit cards, purchasing goods, applying for loans, committing crimes such as murder, theft or other serious crimes, applying for jobs and obtaining documents such as passports or licences.

Online Financial Fraud

Financial fraud occurs when someone steals one's money or harms one's financial health by deceitful, dishonest, or unlawful tactics. This can be accomplished through a variety of means, including identity theft and investment fraud. The modus operandi for each type of financial fraud may differ but one precautionary measure that is common in case of all types of online financial frauds is to be aware and never share sensitive personal information with anyone over text, email or call.

Example: Fraud on fake loan app where a user applied for a loan and was instantly given some small amount money to build trust in exchange for personal information. The victim was then asked to return the money with unbearably high interest within an unreasonable short time frame. After the victim was unable to payback, he was asked to download another fake loan app to repay the previous loan. The cycle goes on and the amount of debt keeps on increasing which the victim has to pay back or else him and his family will be harassed.

[7] Available at https://now.symassets.com/content/dam/norton/campaign/NortonReport/2021/2021_NortonLifeLock_Cyber_Safety_Insights_Report_Global_Results.pdf as accessed on 1-02-2022

Cyber Espionage

Cyber espionage is an act of intrusion or spying that can give the desired information. Traditional espionage, like cyber espionage, is not an act of war, and both are widely considered to be ongoing amongst major countries. Regardless of this presumption, some occurrences can generate severe tensions between states and are frequently referred to as "attacks".

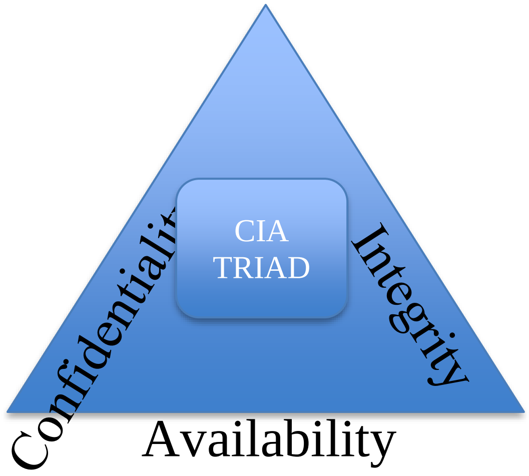
Example: Edward Snowden exposed massive US eavesdropping on numerous countries in 2013. Following the disclosure of the NSA's snooping on German Chancellor Angela Merkel was disclosed, the Chancellor compared the NSA to the Stasi (the official state security service of the German Democratic Republic). Without the consent of the Bahamian government, the NSA records almost every mobile phone conversation in the Bahamas, as do similar operations in Kenya, the Philippines, Mexico, and Afghanistan.

INFORMATION SECURITY

The practice of preventing unauthorized access, use, disclosure, disruption, alteration, inspection, recording, or destruction of data is known as information security. Information can be anything from personal information to social media profiles, cell phone data, biometrics, and so on. As a result, Information Security encompasses a wide range of research areas, including cryptography, mobile computing, cyber forensics, and online social media, among others.

CIA TRIAD

Information security programs are built around three principles, generally referred to as the CIA Triad - Confidentiality, Integrity, and Availability.



Confidentiality: Protection against unauthorised access to data and systems.

Integrity: Protection against unauthorised changes or modifications to data.

Availability: Providing access to authorised users as and when they need.

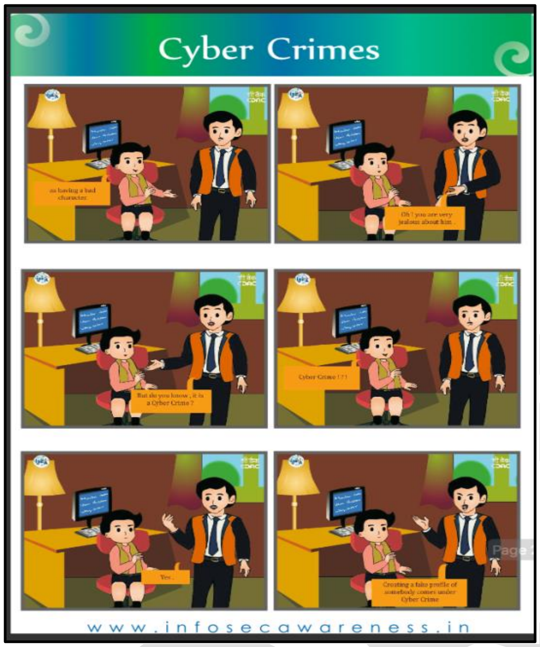
RMIAS MODEL

Information Assurance & Security (IAS) is a dynamic domain that evolves in response to societal, corporate, and technological changes. A Reference Model of Information Assurance and Security (RMIAS) attempts to address recent patterns in the growth of IAS, particularly diversification and de-perimeterization.

The model has four dimensions: the Information System Security Life Cycle, the Information Taxonomy, the Security Goals, and the Security Countermeasures.

CHAPTER 3

TRENDING CYBERCRIMES


Cyber Crimes
as having a bad character.
Oh ! you are very jealous about him .
But do you know , it is a Cyber Crime ?
Cyber Crime ! ? !
Yes .
Creating a fake profile of somebody comes under Cyber Crime
Page
www.infosecawareness.in

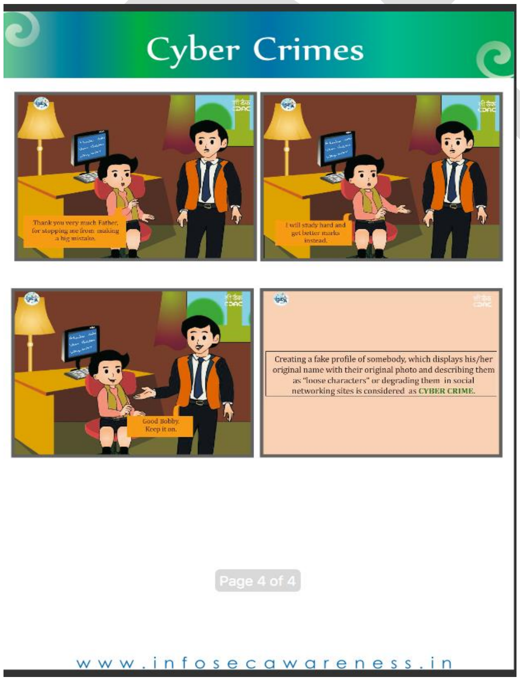
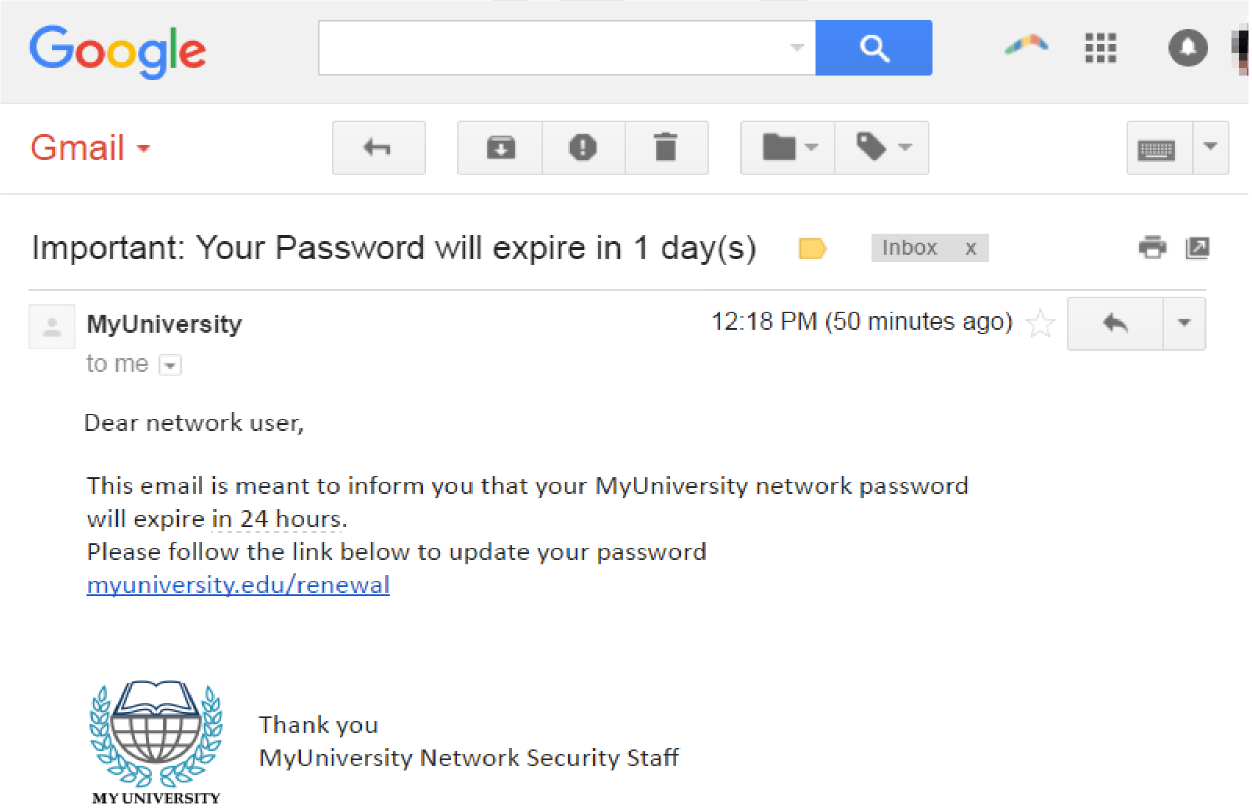

Cyber Crimes
Thank you very much Father, for stopping me from making a big mistake.
I will study hard and get better marks instead.
Good Bobby. Keep it on.
Creating a fake profile of somebody, which displays his/her original name with their original photo and describing them as "loose characters" or degrading them in social networking sites is considered as CYBER CRIME.
Page 4 of 4
www.infosecawareness.in

Fig 1: Cybercrimes

PHISHING

A phishing attack is a means of tricking people into disclosing confidential information by answering an email. It involves obtaining or attempting to gain specific banking information (e.g. username, password, credit card numbers, etc).

Phishing emails and SMS messages may claim to have seen some strange activity or attempted log-ins, assert to have an issue with the account or payment information, ask to verify some personal information, send a fake invoice, demand payment by clicking on a link, show eligibility for a government refund or provide a coupon for free goods.



Important: Your Password will expire in 1 day(s)

MyUniversity 12:18 PM (50 minutes ago)
to me

Dear network user,

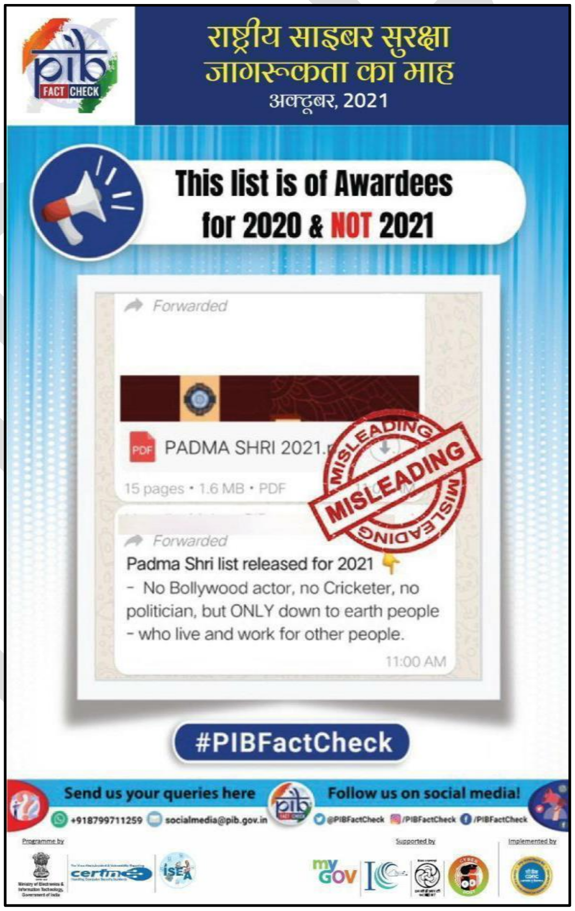
This email is meant to inform you that your MyUniversity network password will expire in 24 hours.
Please follow the link below to update your password
myuniversity.edu/renewal

Thank you
MyUniversity Network Security Staff

Fig.2 Phishing Attack Example

Fake Messages: Scammer’s frame personalized messages posing as people or institutions that one trusts. To make their messages more compelling, they frequently obtain personal information about a person from social media platforms or a hacked account of someone they know.

Example: The Delhi Police's cybercrime unit is warning people about a potential scam in which criminals are duping unsuspecting users by requesting them to verify their phone numbers due to Know Your Customer (KYC) concerns. According to a tweet from the Delhi Police's cyber-crime unit, scammers are sending false messages to consumers saying that their SIM cards will be disconnected if they do not contact the phone numbers provided in the message.



राष्ट्रीय साइबर सुरक्षा
जागरूकता का माह
अक्टूबर, 2021

This list is of Awardees
for 2020 & NOT 2021

Forwarded

PADMA SHRI 2021.p

15 pages • 1.6 MB • PDF

Forwarded

Padma Shri list released for 2021 👇
- No Bollywood actor, no Cricketer, no politician, but ONLY down to earth people
- who live and work for other people.

11:00 AM

#PIBFactCheck

Send us your queries here
+918799711259 socialmedia@pib.gov.in

Follow us on social media!
@PIBFactCheck /PIBFactCheck /PIBFactCheck

Email Phishing: This type of attack tries to steal confidential information by sending an email that appears to be from a trusted organization. It is not a targeted attack and can be carried out in large numbers.

Spear Phishing/Whaling: Sending emails to particular and well-researched victims while posing as a trustworthy sender is known as spear phishing. The goal is to infect devices with malware or persuade victims to divulge personal information or money. Unlike most phishing attacks, spear-phishing is a highly targeted, well-researched attack that primarily targets business executives, public personas, and other valuable targets.

InfoSec for KID CARTOON STORYBOARD
NATIONAL CYBER SECURITY AWARENESS MONTH
OCTOBER, 2021
75 Azadi Ka Amrit Mahotsav
Phishing Attacks
Vicky was very active boy in his school
He love to play Online games and felt them very challenging
One day, he downloaded a game named "Game of kings" and completed the game
A popup came on the screen with download link for the full version of game
He felt its true and clicked on the download link
It redirected him to a page showing a form to fill in the details including the credit card, so he filled his dad's card details
Later, he didn't get any upgrade for the full version of the game
Update to full version
Meanwhile, his dad got a message of amount deduction from his credit card
He asked Vicky whether he used his Credit card without his permission
Vicky apologised and said that he used the card details in a form online for downloading a game
Vicky's dad called the bank customer care for blocking the card and filed a complaint
The bank official immediately responded & blocked the card
cerfmc
isea
www.isea.gov.in
my GOV

Vishing: Vishing, also known as voice phishing, is when a malicious caller poses as tech support, a government agency, or another institution to get sensitive information such as banking or credit card details through a phone call or voice message.

Example: Any call from an unknown source may prove dangerous to the receiver. Especially calls taken with two digits or three digits numbers with the prefix "+".

Fake Websites: This type of cyber fraud comes in a variety of forms. In one, the scammers establish a genuine-looking website for a well-known brand or even a mobile phone company and advertise low-cost products. They trick the unsuspecting buyer into paying online, but the customer never receives the items they bought.

Example: A false website created has a policy whereby if a customer purchases any goods that cost more than a specific amount, he or she will be eligible for a free costly item. As soon as the buyer purchases the product, the buyer receives a call from the fraudulent website's customer service informing the customer to pay a particular refundable amount toward shipping, service, GST, and other aspects of the freebie. As a result, the scammers trick the unsuspecting internet buyer into depositing thousands of rupees into multiple bank accounts.

InfoSec POSTER
NATIONAL CYBER SECURITY AWARENESS MONTH
OCTOBER, 2021
75 Azadi Ka Amrit Mahotsav
Beware of
Fake 'Free Online Offers'
Forwarded
eoffers
30th anniversary celebration
Free gifts for everyone !
Save yourself from possible
Data leaks and Malware attacks
Free gifts
click here
Programme by
cerfme
isea
www.isea.gov.in
Supported by
my Gov
Implemented by

Never believe the free gift offers messages or mails circulated online as bait by fraudsters

Do not forward fake messages/ links/ mails without proper verification or authentication

Never share your personal details or financial information like login credentials/ passwords/credit or debit card details

Never click on unknown links or download unauthorized apps or software on your digital devices

Safe Tips:

Do’s -

- Look for spelling or grammatical mistakes in the email body
- Check the domain name if sent from a public domain email
- Check the authenticity of a message before forwarding it on social media platforms

Don’ts -

- Do not click on suspicious links or attachments
- Do not take phone calls from unknown sources
- Do not login to fake/illegal websites

FINANCIAL FRAUDS

Internet Banking-related Fraud: All banking services are now available online. Online services include accessing account statements, transferring funds to other accounts, getting a cheque book, and producing demand drafts, among others. As more services move to online platforms, cyber fraud in the financial sector is on the rise. This can be done through an attack on digital payments applications, by the hacking of bank accounts due to weak passwords, or by hacking multiple accounts due to the same password.

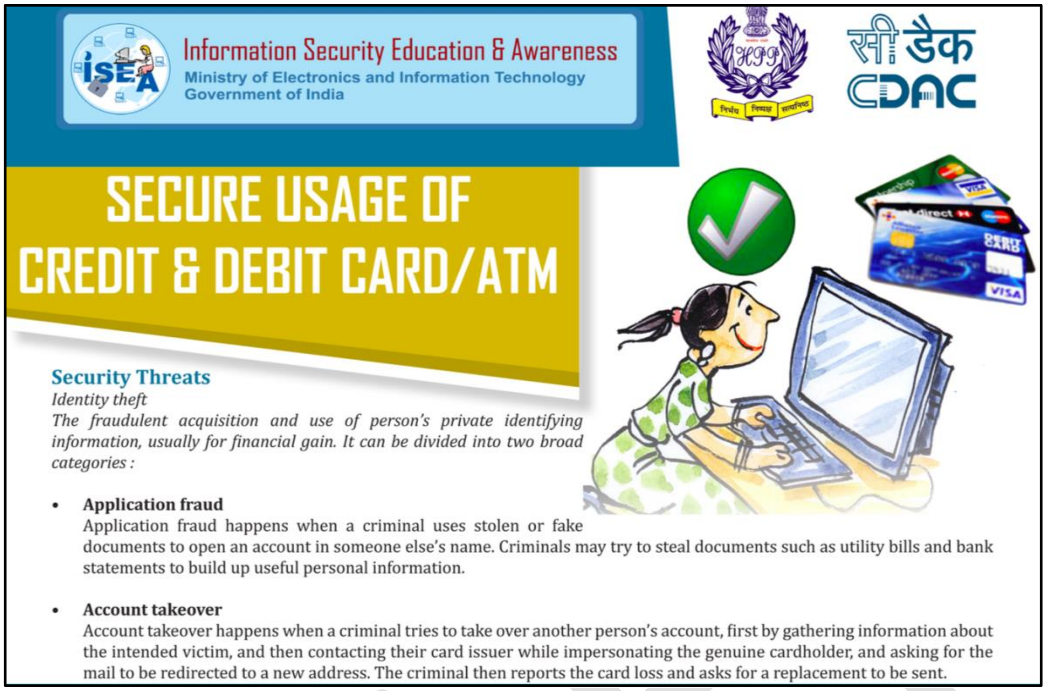
UPI Fraud: It's a frequent method for scammers to deceive people by sending them a payment request over their UPI app. This request makes it simple for them to transfer the money. When the payment request is approved, the UPI app prompts users for the PIN, which is the final step in the process. When a person enters their UPI PIN, they lose all of their earnings.

OTP Fraud: Victims get SMS / Instant messages from fraudsters impersonating as NBFCs offering loans or enhancement of credit limit and are asked to contact the fraudster’s mobile number. When the victims call the number, the fraudsters ask them to fill few forms (even online) containing financial details and they incite / convince them to share the OTP or PIN details, resulting in loss of money. The OTP frauds can also happen after the person has been a victim of social engineering attack where he/she provided the financial details to the attacker via email, etc. and the attacker then initiates a transaction from the victim’s bank account and calls the victim convincing him/her to give the OTP.

E-Wallet Fraud: KYC has been made compulsory for mobile wallet users by the Reserve Bank of India. KYC has been misused by scammers as an access point. Many network service operators send nudges to not fall bait to the KYC-related messages for an account. They deny asking for any personal information through messages or calls.

Example: Typically, the victim receives a text message claiming that the e-wallet requires KYC compliance and that they must call the specified phone number. The person is invited to download an application, usually, TeamViewer Quick Support or AnyDesk, which are remote access control mobile apps, to update their KYC. To check the status of the e-wallet, the scammers ask for a Re. 1 transfer. While the customer is typing in a password or PIN for the e-wallet, the scammers are gathering data. They now have access to the password and ID for the mobile wallet. The wallet is debited to other accounts using separate transactions as the bank account is linked to the phone.

Credit/Debit Card: Frauds using cards and digital transactions are constantly changing. Frauds exploiting credit and debit cards are growing more widespread. Unauthorized use of a credit or debit card or a comparable payment method (ACH, EFT, recurring charge, etc.) to unlawfully obtain money or property is described as credit/debit card fraud. Numbers for credit and debit cards can be taken through insecure websites or obtained through an identity theft scam.


Information Security Education & Awareness
Ministry of Electronics and Information Technology
Government of India
iSEA
सी डैक
CDAC

SECURE USAGE OF CREDIT & DEBIT CARD/ATM

Security Threats

Identity theft

The fraudulent acquisition and use of person's private identifying information, usually for financial gain. It can be divided into two broad categories :

- **Application fraud**
  Application fraud happens when a criminal uses stolen or fake documents to open an account in someone else's name. Criminals may try to steal documents such as utility bills and bank statements to build up useful personal information.
- **Account takeover**
  Account takeover happens when a criminal tries to take over another person's account, first by gathering information about the intended victim, and then contacting their card issuer while impersonating the genuine cardholder, and asking for the mail to be redirected to a new address. The criminal then reports the card loss and asks for a replacement to be sent.

SIM Swap Fraud: SIM swap simply means changing mobile SIM cards. If this is done without the user's permission, it is most likely for fraudulent purposes. SIM swap fraud occurs when scammers obtain a new SIM card from the mobile service provider using the registered phone number. They can acquire One Time Password (OTP) and other alerts needed to execute financial transactions through the bank account with the use of the new SIM.

Sim Cloning: This is basically creating a duplicate SIM from the original one. It is similar to SIM swapping. However, this is a technically sophisticated technique, where software is used to copy the real SIM card. It is done to get access to victims International Mobile Subscriber Identity (IMSI) and encryption key, which are used to identify and authenticate subscribers on mobile telephony. Cloning the SIM will enable the fraudster to take control and track, monitor, listen to calls, make calls and send texts using the mobile number.

Demat/Depository Fraud: The protection of the shares and securities is the responsibility of India's two depositories, CDSL and NSDL. CDSL and NSDL, however, do not deal directly with Demat account holders. They supply stockbrokers and intermediaries with Depository Participant (DP) licenses, which allow consumers to open Demat accounts. For instance, in some cases, brokers have transferred ETF units to use as collateral for margin funds on trades without the permission of investors.

Cryptocurrency Fraud: Due to its fast transactions, mobility, and global reach, cryptocurrency can be used as a new tool for evading taxes, money laundering, and bribery. Fraudsters may try to manipulate the markets for cryptocurrency and similar derivative assets. Spoofing, front-running, churning, and other methods are forms of improper market manipulation. Cryptojacking is a form of cryptocurrency cybercrime in which hackers misuse people's electronic devices such as computers, cellphones, tablets, and even servers to mine for bitcoin without their permission.
Example: Investors' crypto wallets can be hacked, allowing scammers to steal their funds. They can create fake wallets to defraud counterparties, as well as fake crypto exchanges to steal money from clients.

Safe Tips:

Do’s -

- Make a separate email address for online buying to prevent harmful emails disguised as sales promotions.
- Always use an onscreen keyboard to enter password and log out of the banking portal/website after completing an online payment using public computers. Also, remove the browsing history from the web browser.
- Check the seller's reputation and credibility before making online payments.
- When buying a second -hand phone make sure that it does not come with any suspicious pre-installed Apps that may contain malwares.

Don’ts -

- Do not give the net-banking password, One-Time Password (OTP), ATM or phone banking PIN, CVV number, or other sensitive information to anyone, even if they pretend to be a bank employee or representative, and notify the bank if this happens.
- Do not scan any QR codes to receive payments from unknown sources.
- Do not save banking/personal information in a browser or on a payment site while making a purchase.

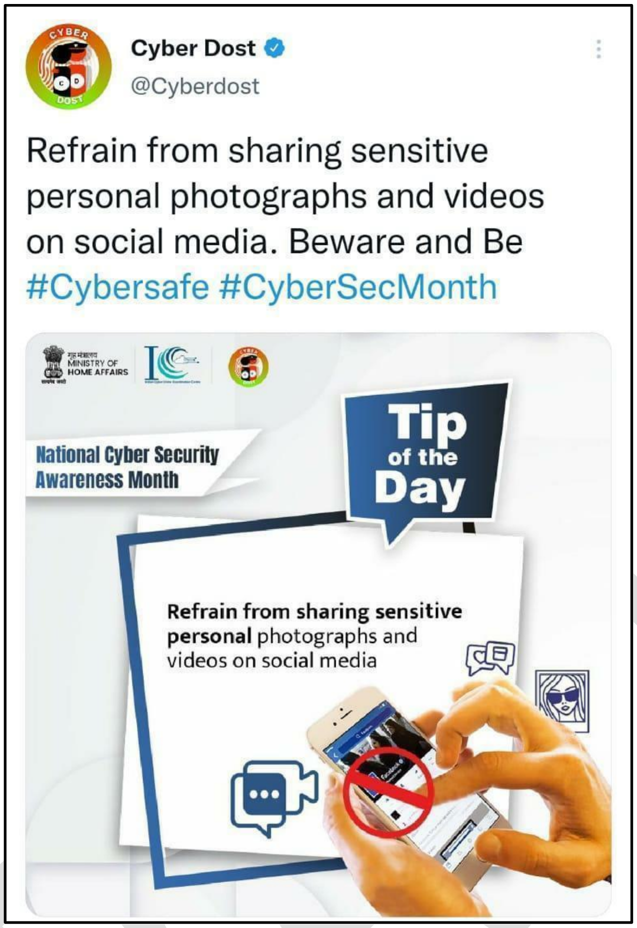
SOCIAL MEDIA CRIMES

Cyberstalking: Cyberstalking is a crime when a victim is harassed by the attacker utilizing e-mail, Instant Messaging (IM), internet messages, discussion groups, etc., to communicate electronically with the victim. A cyberstalker depends on the fact that in the internet realm his real identity is unknown. A cyberstalker targets and follows victims through with threatening/abusive communications.

Example: A boy is stalking a girl on social media and then bothering her by texting on her social media about her online posts..

Cyberbullying: Cyberbullying is bullying through digital technology where the unpleasant, damaging, and wrong content about someone else can be sent, posted, or shared. The purpose is to induce confusion or shame. Users may be able to watch, interact, or share material via SMS, social media, forums, or gaming applications. Cyberbullying poses a risk to those who are socially active on numerous social media platforms.

Sexting: Sexting is defined as sending or sharing sexually provocative text messages and images, including nude or semi-nude photos, via mobile phones or the Internet. These photos and messages are extremely private in nature and if a criminal gets access to these, then it can become a serious problem. This could happen as a result of hacking, in which the photographs are taken from the original receiver, or as a result of the intended receiver spreading them without the sender's permission (either with other friends or in web forums). When photographs are shared without the victim's consent, sexting becomes a concern and the victim is said to have become a prey to a cybercrime. Users/Senders may be unaware that their photographs may be distributed, or a previously trusted recipient may turn out to be unworthy of such trust.



Cyber Dost
@Cyberdost

Refrain from sharing sensitive personal photographs and videos on social media. Beware and Be #Cybersafe #CyberSecMonth

MINISTRY OF HOME AFFAIRS
National Cyber Security Awareness Month
Tip of the Day
Refrain from sharing sensitive personal photographs and videos on social media

Honey Trapping: Honey trapping uses the cyber espionage technique in which a cyberattack occurs through romantic or sexual relationships with civilians whereby the attacker takes advantage of the intimacy in the relationship to coerce or blackmail the victim. The threat actors use this cybercrime to discover or reveal sensitive information.

Trolling: Trolling is defined as intentionally inflicting hatred, discrimination, racism, sexism, or simply arguing with others. It's the anti-social act of provoking online personal disputes and controversy. Trolls are people who engage in trolling behaviors. It was termed "flaming" in the early days of the Internet. Individuals use blog sites, social networks like Facebook, Instagram, and Twitter, news sites, discussion forums, and game chats, as well as any other place that allows them to make public remarks.

Safe Tips:

Do’s -

- Keep social media profiles’ privacy settings as strict as possible, especially for the public/others.
- Exercise extreme caution when sharing anything on the internet.
- Log out after each session.

Don’ts -

- Do not give out social media login information to anyone.
- Do not accept friend requests from strangers.
- Do not click on any links that appear to be suspicious.

MORPHING

Pornography: Pornography is defined as any obscene or sexually explicit information. Pornography is available in a variety of media on the internet. These include images, small animated films, sound files, and stories. The Supreme Court has defined obscene as “offensive to modesty or decency; lewd, filthy, repulsive.”

Revenge Pornography: One of the most serious threats to online modesty or reputation issues is revenge pornography. The behavior could be motivated by a desire to smear the person's morality in public. The person may misuse the individual's identity and converse as a person who is sexually motivated, often pretending to be a call girl, revealing the victim’s real name and photograph. For instance, someone seeking vengeance might either hack into the real accounts or simply make false profiles.

Grooming: Grooming is the way in which somebody may get close to a child, with the intention of sexually exploiting them. Grooming could be done by anyone, of any age or gender, and could be done in person or online. With the advent of Internet and social media, grooming practices have become more common and prevalent. Predators can very easily make a fake profile on any social media platform to appear younger or someone the child may know. Young children between the ages 13 to 15 are especially susceptible to be groomed or manipulated by the adults they meet online. Many countries have laws preventing adults from “corrupting” minors or engaging in sexually explicit conversations with those under the age of 18. In addition, it is illegal to send pornographic to minors or to encourage and pressure minors to send explicit photographs or videos of themselves.

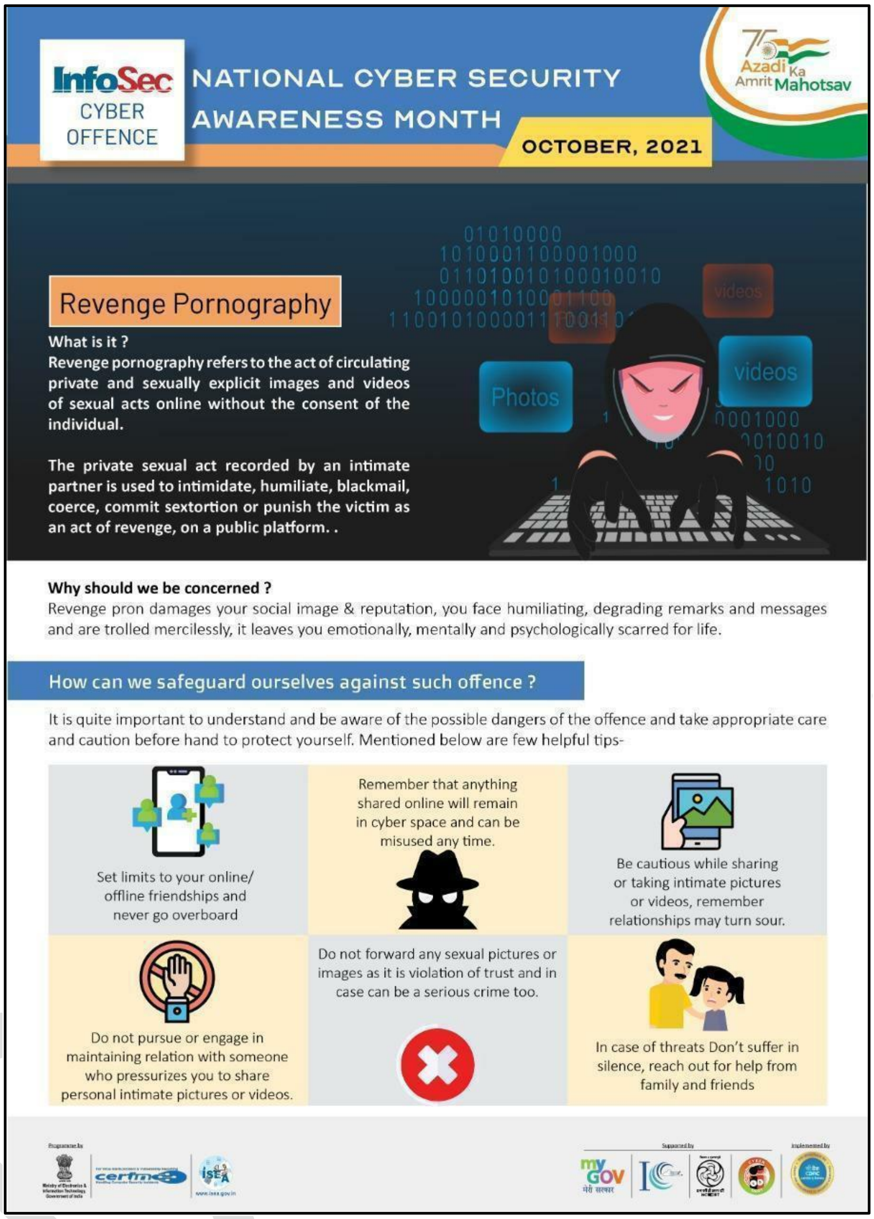
Safe Tips:

Do’s -

- Set limits in online/offline friendships.
- Be cautious while sharing or taking intimate pictures or videos.
- Remember that anything shared online will remain in cyberspace and can be misused anytime.

Don’ts -

- Do not pursue or engage in relationships that pressurize sharing of personal pictures or videos.
- Do not forward any sexual pictures or videos as it can cause a violation of trust.
- Do not suffer in silence, in case of any threats.


Photos
videos
videos
Programme by
Ministry of Electronics & Information Technology Government of India
cert-in
isea
www.isea.gov.in
Supported by
my GOV मेरी सरकार
Implemented by
CDAC

InfoSec CYBER OFFENCE

NATIONAL CYBER SECURITY AWARENESS MONTH

OCTOBER, 2021

75 Azadi Ka Amrit Mahotsav

Revenge Pornography

What is it ?

Revenge pornography refers to the act of circulating private and sexually explicit images and videos of sexual acts online without the consent of the individual.

The private sexual act recorded by an intimate partner is used to intimidate, humiliate, blackmail, coerce, commit sextortion or punish the victim as an act of revenge, on a public platform. .

Why should we be concerned ?

Revenge pron damages your social image & reputation, you face humiliating, degrading remarks and messages and are trolled mercilessly, it leaves you emotionally, mentally and psychologically scarred for life.

How can we safeguard ourselves against such offence ?

It is quite important to understand and be aware of the possible dangers of the offence and take appropriate care and caution before hand to protect yourself. Mentioned below are few helpful tips-

Set limits to your online/ offline friendships and never go overboard

Remember that anything shared online will remain in cyber space and can be misused any time.

Be cautious while sharing or taking intimate pictures or videos, remember relationships may turn sour.

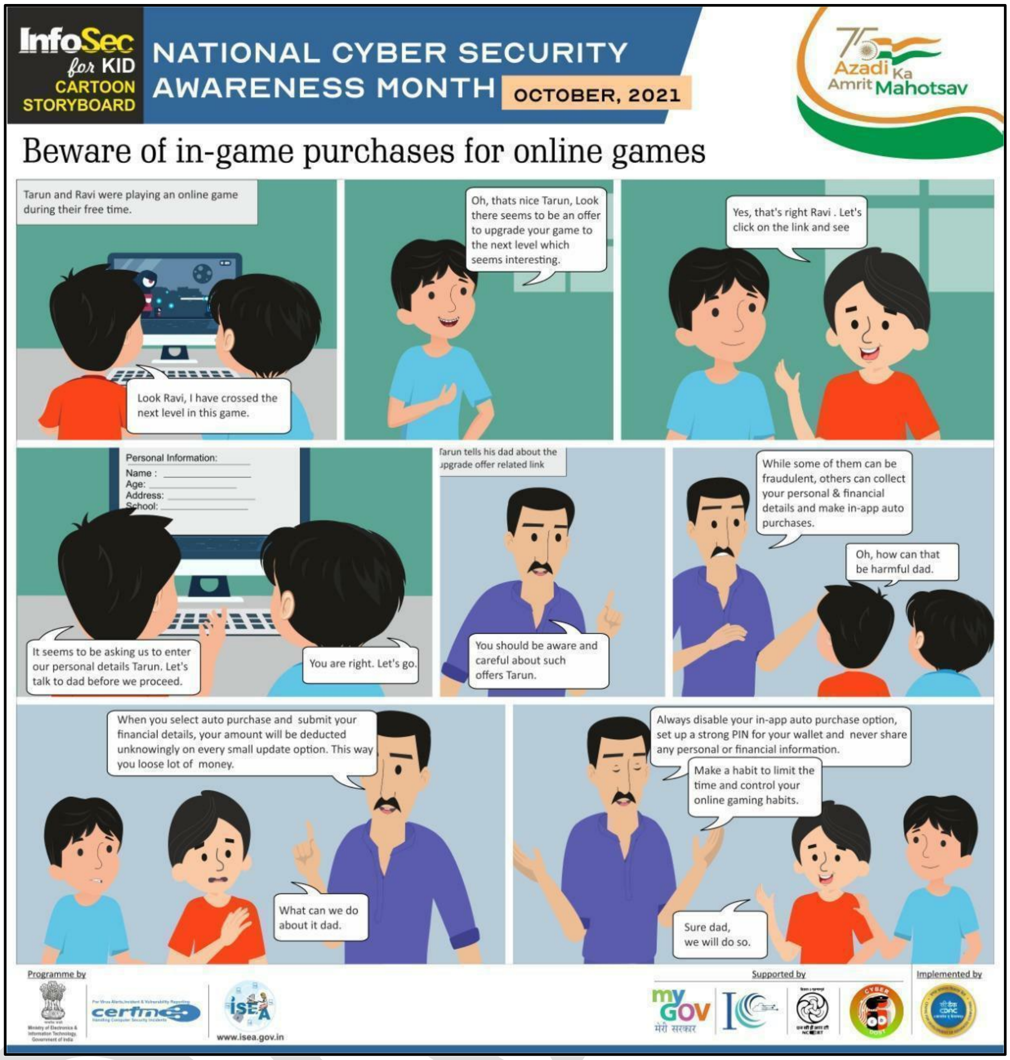
Do not pursue or engage in maintaining relation with someone who pressurizes you to share personal intimate pictures or videos.

Do not forward any sexual pictures or images as it is violation of trust and in case can be a serious crime too.

In case of threats Don't suffer in silence, reach out for help from family and friends

MOBILE APPS

Dangerous game challenges: Anyone who plays an online game or spends more time in online gaming, must know the risks associated with online gaming. In-game resources, well-developed game characters, paid game accounts, or linked credit-card data are potential targets for cybercriminals. These can be taken from users in a variety of ways, including phishing, password-stealing software, and in-game fraud.


InfoSec for KID
CARTOON STORYBOARD
NATIONAL CYBER SECURITY AWARENESS MONTH
OCTOBER, 2021
75 Azadi Ka Amrit Mahotsav
Beware of in-game purchases for online games
Tarun and Ravi were playing an online game during their free time.
Look Ravi, I have crossed the next level in this game.
Oh, thats nice Tarun, Look there seems to be an offer to upgrade your game to the next level which seems interesting.
Yes, that's right Ravi . Let's click on the link and see
Personal Information:
Name :
Age:
Address:
School:
It seems to be asking us to enter our personal details Tarun. Let's talk to dad before we proceed.
You are right. Let's go.
Tarun tells his dad about the upgrade offer related link
You should be aware and careful about such offers Tarun.
While some of them can be fraudulent, others can collect your personal & financial details and make in-app auto purchases.
Oh, how can that be harmful dad.
When you select auto purchase and submit your financial details, your amount will be deducted unknowingly on every small update option. This way you loose lot of money.
What can we do about it dad.
Always disable your in-app auto purchase option, set up a strong PIN for your wallet and never share any personal or financial information.
Make a habit to limit the time and control your online gaming habits.
Sure dad, we will do so.
Programme by
Ministry of Electronics & Information Technology, Government of India
cert-in
www.isea.gov.in
Supported by
my GOV मेरी सरकार
Implemented by
CDAC

Malicious apps: The app which upon installation infects the mobile of the victim withmalicious viruses or spyware trojans or harms the device of the user, and collects the user information by asking for unnecessary access permissions to files, GPS coordinates, e-mail address, contact lists, etc.,and sends it to the third parties.

Case: India's Computer Emergency Response Team (CERT-In) had issued an advisory to bank customers of an android malware that stole information and money. The malicious app disguised as Income Tax Department app and asked the users for permissions to the user's SMS, call logs and contacts. The information included personal details like full name, PAN, Aadhar number, address, date of birth, mobile number, and email address. It also demanded financial information such as account number, IFS code, CIF number, debit card number, expiry date, CVV and PIN. The app then sent all the user’s details to the attacker and rendered a fake update screen to the user.

Matrimonial Frauds: Fraudsters befriend the victim after creating an intriguing online marriage profile on any reputable matrimonial site and posing as a prospective candidate. Through emails, online chats, and sometimes phone calls, they gain trust and get connected to the victim. Fraudsters then propose marriage and, when speaking with the victim they're trying to trick, they use voice-changing applications to impersonate their parents and guardians. Once they have the victim's trust, the scammers urge them to deposit money into their bank accounts, claiming an emergency. They disappear as soon as the payment is made, and the cycle begins again with the next victim.

Career frauds: Another form of fraud is employment-related fraud, as people have started looking for job opportunities online, it has allowed scammers to trick people into scams. Scammers offer fake job opportunities to job seekers through various online services claiming to hold positions in recognized companies and this makes it difficult for people to find out if the offer is legitimate or not.

Safe Tips:

Do’s -

- Look for matrimonial sites or job portals that are genuine and trustworthy.
- Check social media profile on Facebook or LinkedIn of the person who is offering marriage proposal/job.

Don’ts -

- Do not stream or download movies, music, books, or apps from unreliable sources.
- Do not play online games with strangers.
- Do not share personal/financial information with online friends or recruiters.

गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS
CYBER DOST

BEWARE OF FAKE FRIEND REQUEST

Cyber criminals often create fake social media profile to befriend potential victims for obtaining their confidential or personal data

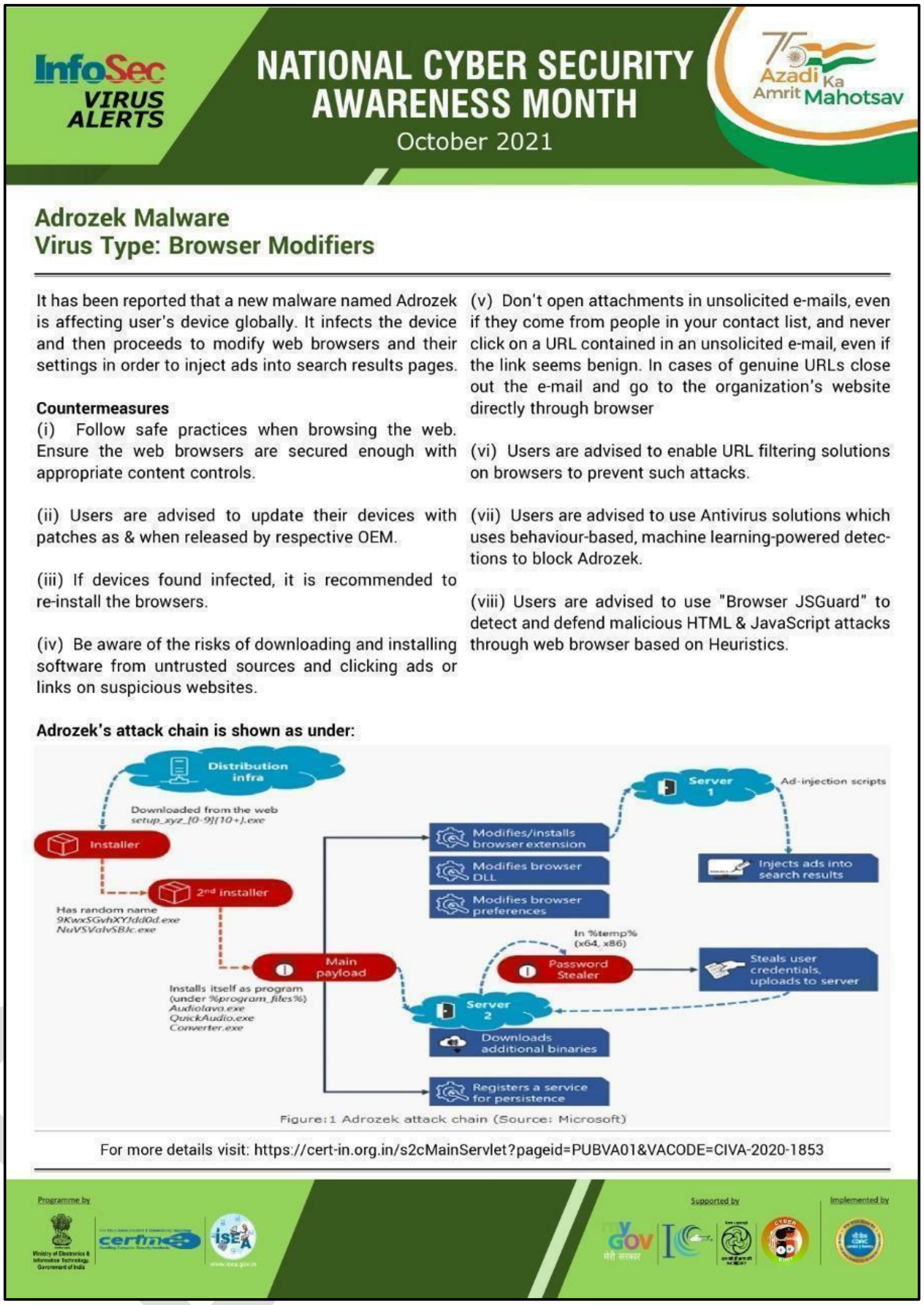
Be careful while accepting online friend request from strangers.

155260
CyberDost
www.cybercrime.gov.in

MALWARE TYPES

Virus

A virus is a kind of malware that replicates itself by inserting its code into other applications. Since the early years of the commercial Internet, computer viruses have been a common threat. Viruses spread through infected websites, flash drives, and emails by attaching themselves to legal files and data. A virus is activated when a victim opens an infected application or file. A virus can erase or encrypt files, alter applications, or disable system functions once it has been actived.



InfoSec VIRUS ALERTS

NATIONAL CYBER SECURITY AWARENESS MONTH

October 2021

Azadi Ka Amrit Mahotsav

Adrozek Malware
Virus Type: Browser Modifiers

It has been reported that a new malware named Adrozek is affecting user's device globally. It infects the device and then proceeds to modify web browsers and their settings in order to inject ads into search results pages.

Countermeasures

(i) Follow safe practices when browsing the web. Ensure the web browsers are secured enough with appropriate content controls.

(ii) Users are advised to update their devices with patches as & when released by respective OEM.

(iii) If devices found infected, it is recommended to re-install the browsers.

(iv) Be aware of the risks of downloading and installing software from untrusted sources and clicking ads or links on suspicious websites.

(v) Don't open attachments in unsolicited e-mails, even if they come from people in your contact list, and never click on a URL contained in an unsolicited e-mail, even if the link seems benign. In cases of genuine URLs close out the e-mail and go to the organization's website directly through browser

(vi) Users are advised to enable URL filtering solutions on browsers to prevent such attacks.

(vii) Users are advised to use Antivirus solutions which uses behaviour-based, machine learning-powered detections to block Adrozek.

(viii) Users are advised to use "Browser JSGuard" to detect and defend malicious HTML & JavaScript attacks through web browser based on Heuristics.

Adrozek's attack chain is shown as under:

Figure:1 Adrozek attack chain (Source: Microsoft)

For more details visit: https://cert-in.org.in/s2cMainServlet?pageid=PUBVA01&VACODE=CIVA-2020-1853

Programme by

Ministry of Electronics & Information Technology Government of India

Supported by

Implemented by

Worm

A worm virus is a harmful program that duplicates itself and spreads through a network automatically. The worm virus exploits flaws in the security software to steal important information, install backdoors that can be exploited to access the system, corrupt files, and perform other types of harm, according to this definition of computer worm. Worms use up a lot of memory and take up a lot of bandwidth. As a result, servers, individual systems, and networks get overworked and fail.

Trojan

A Trojan horse, often known as a Trojan, is malicious software that appears to be legal yet can take control of the computer. A Trojan is a computer program that is designed to hurt, disrupt, steal, or otherwise harm the data or network. To deceive the user, a Trojan tries to portray itself as a legitimate application or file. Viruses can execute and replicate. A Trojan is unable to do so. Trojans must be executed by the user and this is the reason it comes attached to an executable file

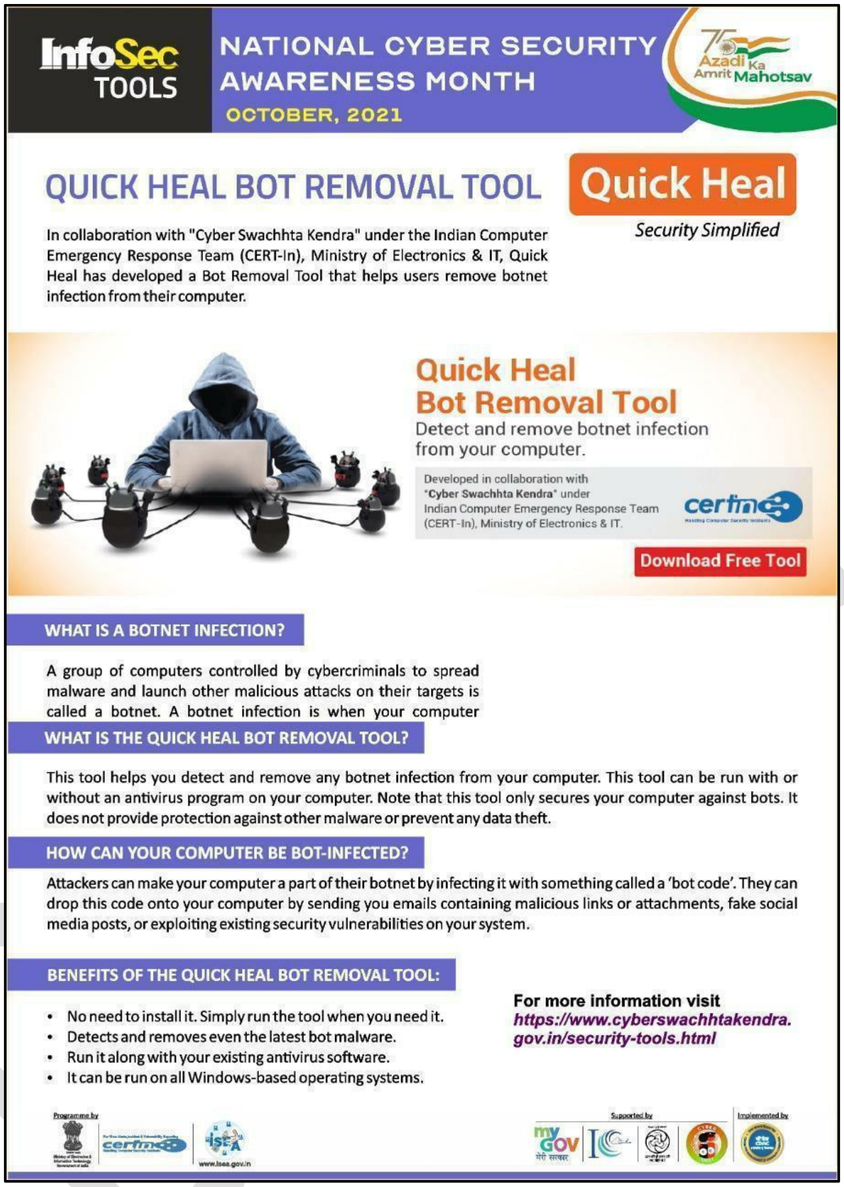
Example: You downloaded an executable file thinking it's a game you need to install but with it a Trojan Horse has also been attached. Once you run that exe file, along with the game, the Trojan also gets installed on your computer and the attacker gets access to your device remotely.

Rootkits

A rootkit is a kind of software that allows hackers to gain access to and command over a computer. Although most rootkits attack software and the operating system, some can also infect the hardware and firmware of the machine. Rootkits are good at hiding their presence, yet they are still active when they are hidden. Rootkits allow hackers to steal sensitive data and financial information, install malware or utilize computers as part of a botnet to send spam and participate in DDoS (distributed denial of service) attacks once they get unauthorized access to computers.

Bots

A bot is a computer program that performs automatic, repetitive, and pre-defined activities. Bots are designed to mimic or replace human behavior. They are significantly faster than human users since they are automated. They do essential tasks like customer support or indexing search engines, but they may also be malware, which is used to take complete control of a computer. Companies and Individuals employ bots to do repetitive activities that would otherwise be performed by humans. When compared to human effort, bot tasks are usually simple and completed at a considerably faster rate. These bots are sometimes used for illegal operations including data theft, frauds, and DDoS assaults.



InfoSec TOOLS

NATIONAL CYBER SECURITY AWARENESS MONTH

OCTOBER, 2021

75 Azadi Ka Amrit Mahotsav

QUICK HEAL BOT REMOVAL TOOL

Quick Heal

Security Simplified

In collaboration with "Cyber Swachhta Kendra" under the Indian Computer Emergency Response Team (CERT-In), Ministry of Electronics & IT, Quick Heal has developed a Bot Removal Tool that helps users remove botnet infection from their computer.

Quick Heal
Bot Removal Tool

Detect and remove botnet infection from your computer.

Developed in collaboration with "**Cyber Swachhta Kendra**" under Indian Computer Emergency Response Team (CERT-In), Ministry of Electronics & IT.

cert-in

Download Free Tool

WHAT IS A BOTNET INFECTION?

A group of computers controlled by cybercriminals to spread malware and launch other malicious attacks on their targets is called a botnet. A botnet infection is when your computer

WHAT IS THE QUICK HEAL BOT REMOVAL TOOL?

This tool helps you detect and remove any botnet infection from your computer. This tool can be run with or without an antivirus program on your computer. Note that this tool only secures your computer against bots. It does not provide protection against other malware or prevent any data theft.

HOW CAN YOUR COMPUTER BE BOT-INFECTED?

Attackers can make your computer a part of their botnet by infecting it with something called a 'bot code'. They can drop this code onto your computer by sending you emails containing malicious links or attachments, fake social media posts, or exploiting existing security vulnerabilities on your system.

BENEFITS OF THE QUICK HEAL BOT REMOVAL TOOL:

- No need to install it. Simply run the tool when you need it.
- Detects and removes even the latest bot malware.
- Run it along with your existing antivirus software.
- It can be run on all Windows-based operating systems.

For more information visit
https://www.cyberswachhtakendra.gov.in/security-tools.html

Malware bots and internet bots can be programmed to breach user accounts, search the internet for contact information, transmit spam, and do other malicious actions. Attackers may deploy harmful bots in a botnet – a bot network – to carry out these assaults and conceal the source of the attack activity. A botnet is a collection of internet-connected devices that individually run one or more bots, frequently without the device owners' knowledge.

Malware is distributed in the form of a download via social media or email communications that instruct the victim to click a link. The link is frequently in the form of an image or a video, both of which include viruses and other malware. A bot might potentially show up as a warning stating that if the user does not click on the connected link, the machine will be infected with a virus. By clicking the link, the user can infect the machine with a virus.

DAMAGE TO COMPUTER SYSTEMS

Unauthorized access - Unauthorized Access refers to the unauthorized attempts to bypass the security mechanisms of a computer/information system or network.

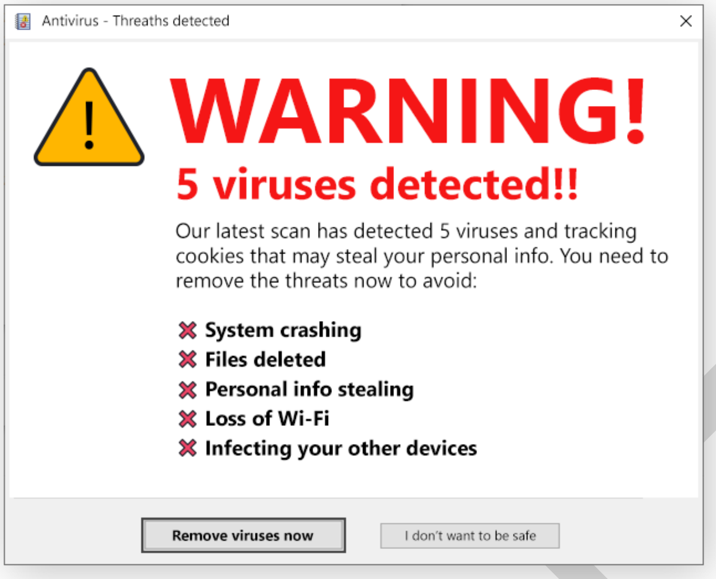
Data breach - A data breach is a security threat in which malicious insiders or external attackers gain unauthorized access to confidential data or sensitive information such as medical records, financial information or personally identifiable information (PII) and so on.

Some other cybercrime and related instances

IoT attacks –IOT attacks include any cyberattacks that seek to gain access to (or control over) IOT devices with the intent to either cause harm to the devices or use them in attacks against other targets.

Advanced persistent threat - An advanced persistent threat (APT) is a broad term used to describe an attack in which an intruder, or team of intruders, establishes an illicit, long-term presence on a network in order to mine highly sensitive data.

Scareware - Scareware is malicious software that tricks computer users to visit malware infected websites or infested websites. Example-scareware may come in the form of pop-ups.



WARNING!

5 viruses detected!!

Our latest scan has detected 5 viruses and tracking cookies that may steal your personal info. You need to remove the threats now to avoid:

- ✖ System crashing
- ✖ Files deleted
- ✖ Personal info stealing
- ✖ Loss of Wi-Fi
- ✖ Infecting your other devices

Adware

Adware is software that displays unwanted (and sometimes irritating) pop-up adverts which can appear on your computer or mobile device. normally comes in software/programmes that you download from the internet – usually freeware or shareware – and it secretly installs itself onto your device without your knowledge.

Free software which contains some ads may be annoying but is not illegal. However, if a third-party programme adds malicious ad software onto your device without your consent, then it is illegal. Adware typically ends up on a user’s device through one of two ways:

You might install a free computer program or app without necessarily realizing that it contains additional software that contains adware. This allows the app developer to make money but means you could download adware onto your systems without necessarily consenting.

Alternatively, there may be a vulnerability in your software or operating system which hackers exploit to insert malware, including some types of adware, into your system.

CHAPTER 4

A READY RECKONER TO STAY CYBER SAFE

Do’s -

- Use caution and avoid signing in to personal or professional accounts such as e-mail or banking, while using a public Wi-Fi network.
- Install Web Browser with HTTPS enforcement.
- Install a reliable anti-virus software.
- One can use a Virtual Private Network (VPN) on their phone as a hotspot.
- Use a password manager - A password manager is an app or a program that collects and stores all the passwords in one location. To gain access to these passwords, one only needs a master key password.
- One must use AePS, a bank-led system that enables online inter-operable financial inclusion transactions at the PoS (Micro ATM) through any bank's business correspondent using Aadhaar verification.

Educate the kids for not sharing any information related to sensitive and financial aspects at social networks and maintain privacy.

Secure E-commerce usage –

By the service providers:

E-Commerce security refers to the practices that provide secure online transactions. It contains protocols that protect people who make purchases of goods and services on the internet.

- To strengthen the security, it's a good idea to use many security layers. DDoS threats and infectious incoming traffic can be blocked by a Content Delivery Network (CDN). To avoid harmful traffic, machine learning can be used.

- Use SSL Certificates. One of the most important features of SSL Certificates is that they encrypt sensitive data sent over the internet. It ensures that only the intended receiver gets the information.

- To block untrusted networks and control the inflow and outflow of web traffic, use effective e-commerce software and plugins. They should have selective permeability, allowing only trusted traffic to pass.

Measures to be taken by the consumers:

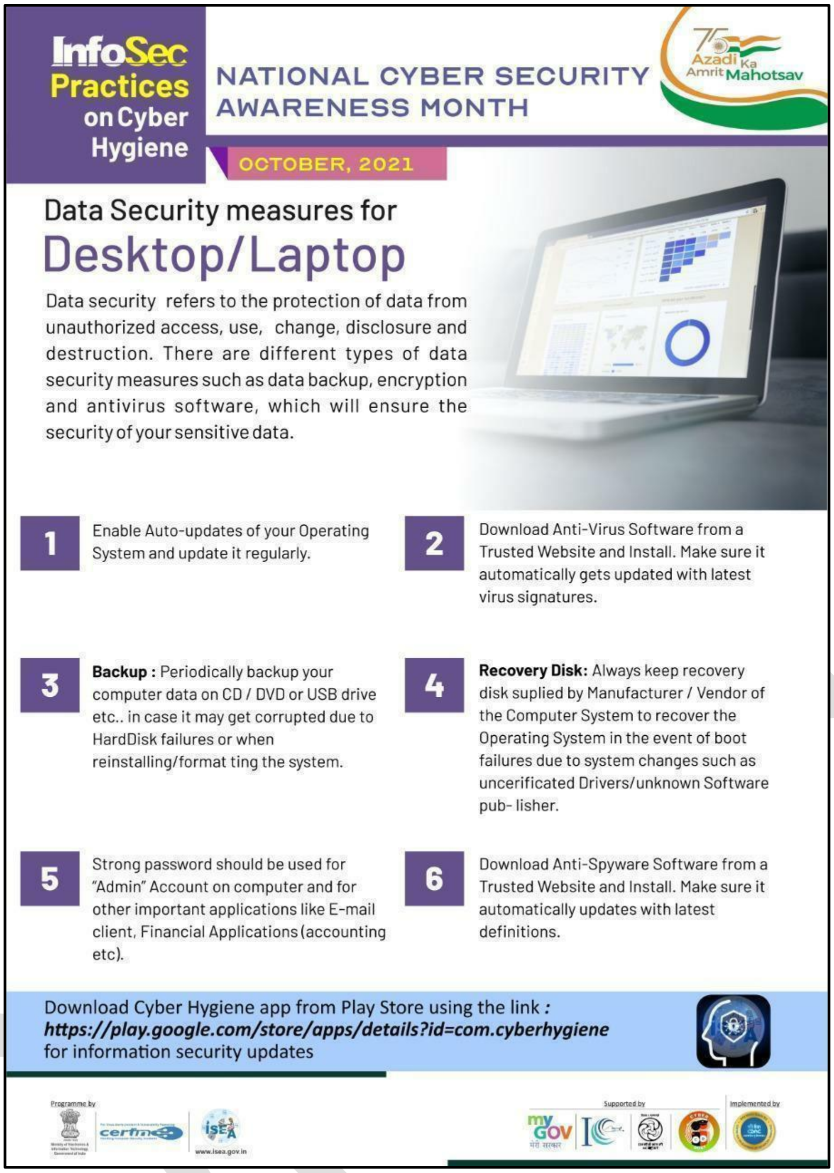
- Install a program or software that detects and blocks harmful software, often known as malware, is required for electronic devices, computer systems, and online systems. Anti-malware software is a type of protection software. All hidden viruses on the website should be rendered by effective anti-malware.
- Always check that the websit starts with HTPPS.

- Do not go blindly on reviews. Look for websites that are genuine and trustworthy.

- Do not trust the customer care numbers provided on google with personal information. They might not always be trustworthy.

Secure computer/laptop usage -

- Use a firewall
- Use the latest antivirus software
- Close the webcam and computer audio when not in use
- Clear browsing history and browser cache from time to time to prevent the use of old forms, protect personal information and help applications run better
- To keep the software up to date, make sure to turn on automatic updates under the settings.
- Set up automatic updates for non-Microsoft software as well such as browsers, Adobe Acrobat Reader, and other programs that are used frequently.
- Do not use a USB or other external device, owned by some other person. Ensure that any external devices either belong to the owner or come from a reliable source to avoid infection by malware and viruses.
- Passwords for logins are important for preventing unauthorized access to the data during boot-up. Setting a password-protected lock screen on the laptop is a smart idea if it is frequently used in public places, such as an office.



InfoSec Practices on Cyber Hygiene

NATIONAL CYBER SECURITY AWARENESS MONTH

75 Azadi Ka Amrit Mahotsav

OCTOBER, 2021

Data Security measures for

Desktop/Laptop

Data security refers to the protection of data from unauthorized access, use, change, disclosure and destruction. There are different types of data security measures such as data backup, encryption and antivirus software, which will ensure the security of your sensitive data.

1 Enable Auto-updates of your Operating System and update it regularly.

2 Download Anti-Virus Software from a Trusted Website and Install. Make sure it automatically gets updated with latest virus signatures.

3 **Backup :** Periodically backup your computer data on CD / DVD or USB drive etc.. in case it may get corrupted due to HardDisk failures or when reinstalling/format ting the system.

4 **Recovery Disk:** Always keep recovery disk suplied by Manufacturer / Vendor of the Computer System to recover the Operating System in the event of boot failures due to system changes such as uncerificated Drivers/unknown Software pub- lisher.

5 Strong password should be used for "Admin" Account on computer and for other important applications like E-mail client, Financial Applications (accounting etc).

6 Download Anti-Spyware Software from a Trusted Website and Install. Make sure it automatically updates with latest definitions.

Download Cyber Hygiene app from Play Store using the link :
https://play.google.com/store/apps/details?id=com.cyberhygiene
for information security updates

Programme by

cerfm

ISEA

www.isea.gov.in

Supported by

my GOV

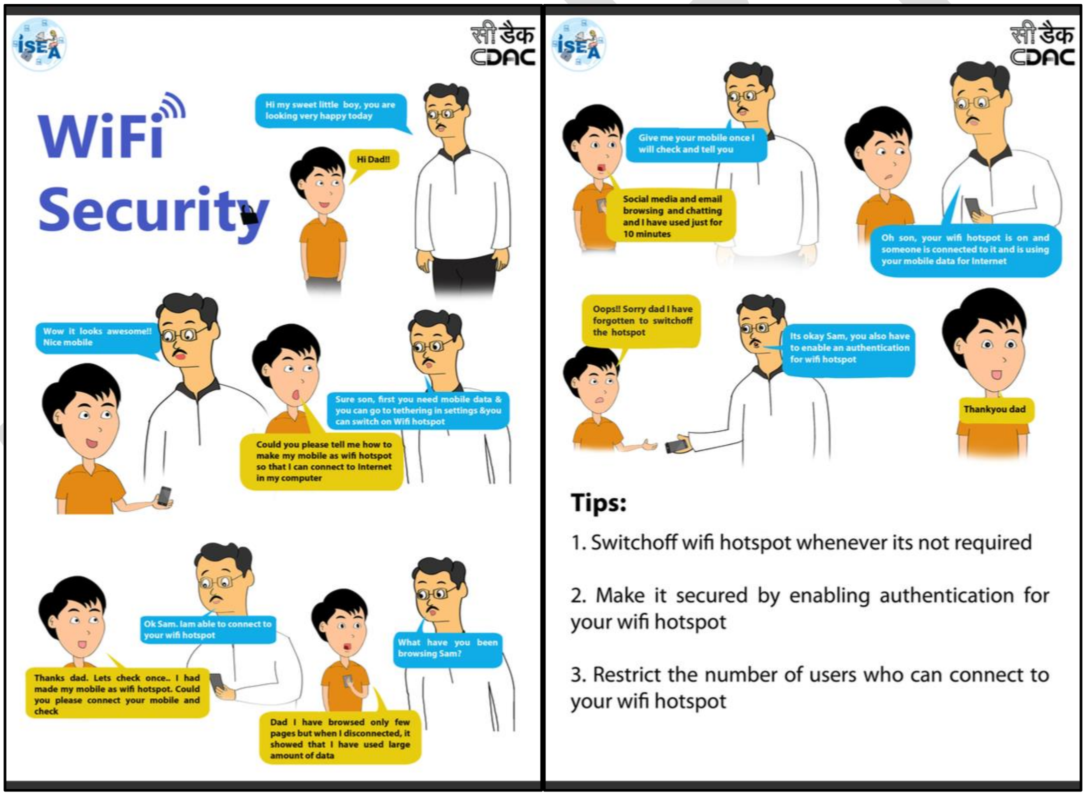
Implemented by

Secure Mobile phone Practices -

● The first step is to ensure that all of the smartphones have screen locks enabled and that entering them requires a password or PIN since the devices have a plethora of personal information.

● Make sure the mobile phones' automatic software upgrades are turned on by default. Updating the operating system regularly guarantees users have the most up-to-date security configurations.

- Do not use public Wi-Fi networks to download videos or content. This increases the risk of exposure to malware and viruses. Delete unused Wi-Fi networks.
- Use a password manager to not only remember the passwords for different accounts but also to generate strong unique passwords for all accounts such as bank accounts, social media, etc.
- Make a backup of the phone data to be able to rapidly access any data that has been compromised if any device is lost or stolen.
- Install the minimum necessary applications and only those from official app stores. Personal information given into applications should be treated with caution.
- When not using location services, turn them off. Do not switch them on in sensitive settings.
- Pop-ups that appear unexpectedly are typically harmful. Close all applications forcibly if one emerges.


ISEA
सी डैक
CDAC
WiFi Security
Hi my sweet little boy, you are looking very happy today
Hi Dad!!
Wow it looks awesome!! Nice mobile
Could you please tell me how to make my mobile as wifi hotspot so that I can connect to Internet in my computer
Sure son, first you need mobile data & you can go to tethering in settings &you can switch on Wifi hotspot
Thanks dad. Lets check once.. I had made my mobile as wifi hotspot. Could you please connect your mobile and check
Ok Sam. Iam able to connect to your wifi hotspot
What have you been browsing Sam?
Dad I have browsed only few pages but when I disconnected, it showed that I have used large amount of data
ISEA
सी डैक
CDAC
Give me your mobile once I will check and tell you
Social media and email browsing and chatting and I have used just for 10 minutes
Oh son, your wifi hotspot is on and someone is connected to it and is using your mobile data for Internet
Oops!! Sorry dad I have forgotten to switchoff the hotspot
Its okay Sam, you also have to enable an authentication for wifi hotspot
Thankyou dad

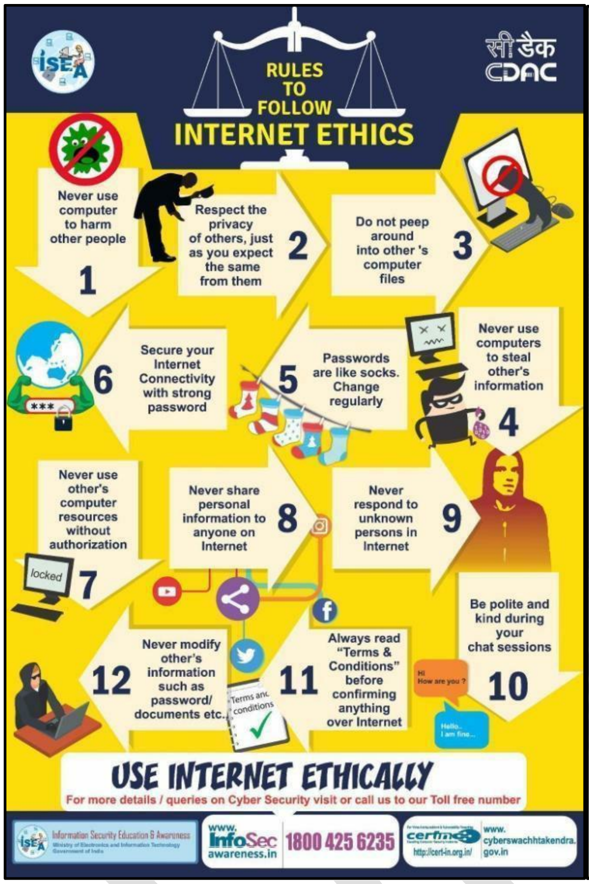
Tips:

1. Switchoff wifi hotspot whenever its not required
2. Make it secured by enabling authentication for your wifi hotspot
3. Restrict the number of users who can connect to your wifi hotspot

Secure Internet Browsing

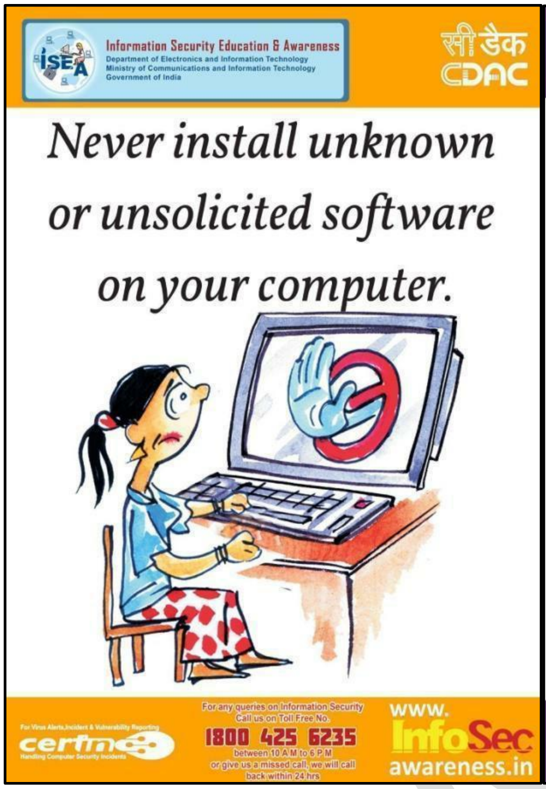
- Be aware of what is being accessed or downloaded. Software should always be downloaded from a reliable source.

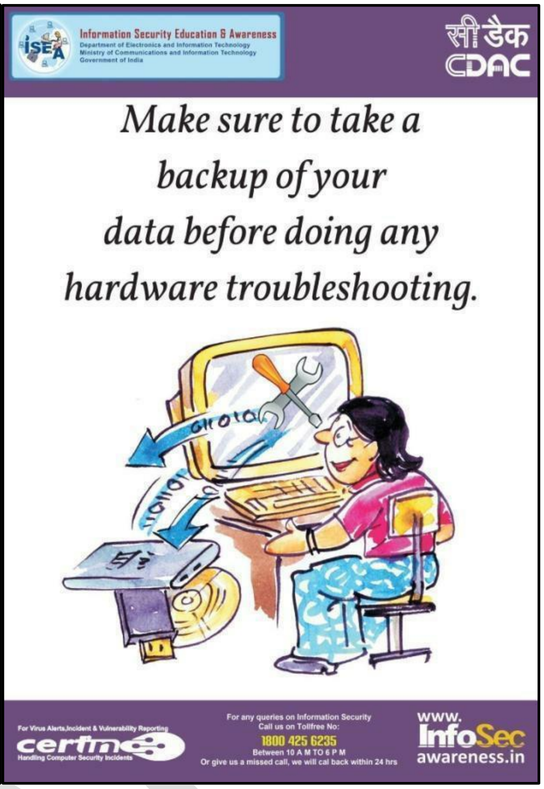
- Before opening any email or clicking a link, double-check the senders' identities.
- Do not save official data to the cloud or on devices that are connected to the Internet.??
- Stay away from services that demand location or ask for upload of photos with GPS coordinates.
- Free downloading software should be avoided at all costs.



RULES TO FOLLOW
INTERNET ETHICS
सी डैक CDAC
Never use computer to harm other people 1
Respect the privacy of others, just as you expect the same from them 2
Do not peep around into other 's computer files 3
Never use computers to steal other's information 4
Passwords are like socks. Change regularly 5
Secure your Internet Connectivity with strong password 6
Never use other's computer resources without authorization 7
locked
Never share personal information to anyone on Internet 8
Never respond to unknown persons in Internet 9
Be polite and kind during your chat sessions 10
Hi How are you ?
Hello.. I am fine...
Always read "Terms & Conditions" before confirming anything over Internet 11
Terms and conditions
Never modify other's information such as password/ documents etc. 12
USE INTERNET ETHICALLY
For more details / queries on Cyber Security visit or call us to our Toll free number
Information Security Education & Awareness
Ministry of Electronics and Information Technology Government of India
www.InfoSec awareness.in
1800 425 6235
cert-in http://cert-in.org.in/
www.cyberswachhtakendra.gov.in

Information Security Education & Awareness
Department of Electronics and Information Technology
Ministry of Communications and Information Technology
Government of India
सी डैक CDAC
Never send your photos through E-mail to Cyberpals & Strangers
Never Respond to Unknown Persons in Internet
For Virus Alerts,Incident & Vulnerability Reporting
cert-in Handling Computer Security Incidents
For any queries on Information Security
Call us on Tollfree No:
1800 425 6235
Between 10 A M TO 6 P M
Or give us a missed call, we will cal back within 24 hrs
www.InfoSec awareness.in


Information Security Education & Awareness
Department of Electronics and Information Technology
Ministry of Communications and Information Technology
Government of India
सी डैक
CDAC
Never install unknown or unsolicited software on your computer.
For Virus Alerts,Incident & Vulnerability Reporting
certin
Handling Computer Security Incidents
For any queries on Information Security Call us on Toll Free No.
1800 425 6235
between 10 A M to 6 P M
or give us a missed call, we will call back within 24 hrs
www.InfoSecawareness.in


Information Security Education & Awareness
Department of Electronics and Information Technology
Ministry of Communications and Information Technology
Government of India
सी डैक
CDAC
Make sure to take a backup of your data before doing any hardware troubleshooting.
01010
For Virus Alerts,Incident & Vulnerability Reporting
certin
Handling Computer Security Incidents
For any queries on Information Security Call us on Tollfree No:
1800 425 6235
Between 10 A M TO 6 P M
Or give us a missed call, we will cal back within 24 hrs
www.InfoSecawareness.in

In Case of Lost Mobile Phones

- Call the cell phone from a different device. One can also sound an alert by using the carrier's mobile app to override ringtone settings.
- If the phone's text messages are enabled to appear on the lock or home screen, leave a text with contact information in case someone finds it.
- Each phone has built-in security settings. One can monitor, ring, lock, or wipe the phone remotely using the ‘find my phone’ feature if it is enabled.
- If a person is quite convinced that the phone has been stolen, one should wipe the data from it remotely as quickly as possible to keep personal information safe.
- If one cannot find the phone fast, use the ‘find my phone’ option on the phone to lock it remotely from anywhere. Also, just in case, change the passwords on all accounts including financial accounts, emails, and social media.
-
- Block the phone’s IMEI by any of the following means:

- Through a form submitted on the website https://www.ceir.gov.in/ The procedure to do it is as follows: -

a) File a report with the police, and keep a copy of the report.
b) Get a duplicate SIM Card for the lost number from your telecom service provider (eg, Airtel, Jio, Voda/Idea, BSNL, MTNL etc.). This is essential because you will need to provide this as the primary mobile number (OTP will be sent on this number) while submitting the request for blocking your IMEI. **Note:** As per TRAI's regulation, SMS facility on re-issued SIMs is enabled after 24 hours of SIM activation.
c) Get your documents ready - a copy of police report and an Identity Proof must be provided. You can also provide the mobile purchase invoice.
d) Fill out the request registration form for blocking the IMEI of lost/stolen phone, and attach the required documents.
e) After submitting the form, you will be given a Request ID. The same can be used for checking the status of your request and for unblocking the IMEI in future.

- Through TSP’s specified customer outlets by contacting the network service operator online. They can turn off the phone's service and, in most cases, make it inaccessible, even if the person uses a new SIM card or switches operators.
- Through State Police by filing a First Information Report (FIR) at the nearest police station. This is also necessary because even if the person may not get the phone back, he/she can at least fight fraudulent charges made with their device.

PREVENTIVE MEASURES

Antivirus

Antivirus software is a type of application that is meant to prevent, detect, and eradicate malware attacks on individual computing devices, networks, and information technology systems. Antivirus software, which was initially meant to identify and remove viruses from computers, can now guard against a wide range of threats, including keyloggers, browser hijackers, Trojan horses, worms, rootkits, spyware, adware, botnets, and ransomware.

Antivirus software generally operates in the background, checking PCs, servers, or mobile devices for malware and limiting its spread. Many antivirus software packages feature real-time threat detection and prevention to defend against potential vulnerabilities as they occur, as well as system scans that check device and system data for potential threats.

Antivirus software often performs the following fundamental functions:

→ Scanning directories or files for known harmful patterns that indicate the existence of malicious malware.

→ Running a scan when a new device is inserted into the computer system.

→ Allowing users to schedule scans for automatic execution.

→ Allowing users to start new scans at any moment, as well as removing any harmful software detected. Some antivirus software applications do this automatically in the background, while others warn users of infestations and prompt them to delete the files.

→ To scan computers thoroughly, antivirus software is typically granted privileged access to the whole system.

As a result, antivirus software is a frequent target for attackers, and in recent years, researchers have uncovered remote code execution and other severe flaws in antivirus software programs. Hence, it is absolutely necessary to get a reputed and reliable antivirus software, and update it regularly from its official site as the company comes out with patches against the latest discovered vulnerabilities.

InfoSec DAILY TIP

NATIONAL CYBER SECURITY AWARENESS MONTH

OCTOBER, 2021

Update your system antivirus as per schedule and avoid delays to ensure system safety.

शेड्यूल के अनुसार अपने सिस्टम एंटीवायरस को अपडेट करें और सिस्टम सुरक्षा सुनिश्चित करने में देरी से बचें।

Firewall

A firewall is a network security device, either hardware or software-based, that monitors all incoming and outgoing traffic and allows, rejects, or drops that specific traffic depending on a predetermined set of security rules.

The networks are changing and developing on a regular basis to adapt to new situations such as reorganization, acquisition, outsourcing, fusion, joint ventures, and strategic partnerships, and the increasing degree of internet connectivity in internal networks. The increasing complexity and openness of the network makes it more complex than before for the security issue and requires the development of advanced security technologies at the interface of networks in various security fields such as between Intranet, the Internet, or Extranet.

A firewall can be the best way to ensure interface safety. The firewall checks network traffic against the rule set defined in its table. When the rule is matched, the associated action is applied to the network traffic.

Passwords

Passwords are one of the most important aspects of the cyber world. From a social media account to a bank login, one requires a password for everything whether it's for accessing the device or for any WiFi. Passwords act as a deterrent against cyber attackers who may try to gain access to the accounts or devices and steal the data. It is very important to store all the passwords in a very secure place. Also, one should have a very strong password which should be difficult to crack and update frequently.

Following are some of the best practices to consider while setting up and managing a password:

a) Create strong password with a minimum length of ideally 10 characters and comprising of mix of alphabets, numbers and characters.

b) All passwords (e.g., email, computer, etc.) should be changed periodically at least once every three months.

c) Don’t reuse old passwords.

d) Passwords should not be stored in readable form in computers, notebook, notice board or in any other location where unauthorized persons might discover or use them.

e) Treat passwords as sensitive information and do not share it with anyone.

f) Always use different passwords for every log-in accounts you have. Using the same password for more than one account risks multiple exposures if one site you use is hacked.

g) If your work requires you to communicate passwords, such as while sending password for an encrypted file sent as an attachment through email it must be communicated through a different channel such as over a phone call or SMS.

h) Always decline the use of the "Remember Password" feature wherever it is prompted by the applications.

i) Remember weak passwords have the following characteristics:

   i. The password contains less than 10 characters

   ii. The password is a word found in a dictionary (English or foreign)

   iii. The password is a common usage word such as: Names of family, pets, friends, colleagues, Movie / Novel / Comics characters, etc. Computer terms and names, commands, sites, companies, hardware, software.

   iv. Birthdays and other personal information such as addresses and phone numbers.

   v. Word or number patterns like 123456, aaaaa, qwerty, asdfg, zxcvb, etc.

j) Some suggested way to construct a strong password are as follows,

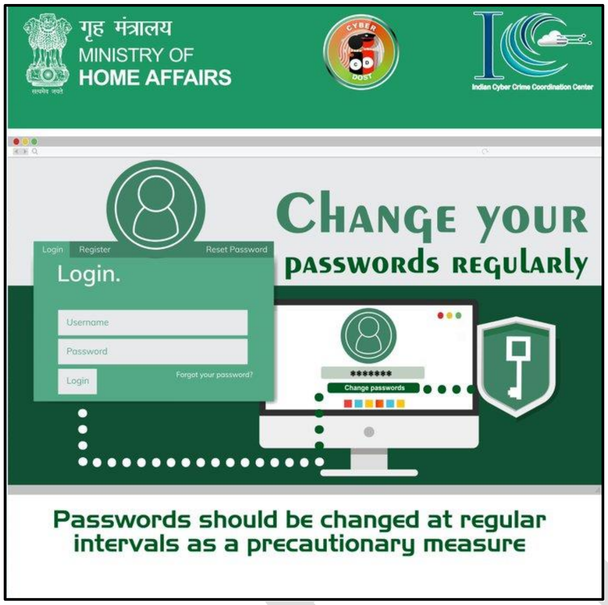
   i. A secure password not only consist of letters, must also use numbers, special characters and caps. One suggested way to replace letters with numbers and special characters, so an “i” will become “!”, an “o” turns into a “0” and “s” is written as “$”. This way, the simple term “Microsoft” changes to the substantially harder word “M!cr0$0ft”.

   ii. Password length matters, the longer the password, the harder it is to crack.

   iii. Think of a sentence and select the first letters of each word in a row will get a complex password and easy to remember as well.

For example, sentence like this, “My Name is Dinesh Anandan and I was born on 1 January 1986!” would produce the following password: “MNiDAaIwbo1J1986!”. It‟s long, contains numbers, special characters, caps and letters, and it‟s easy to remember and won‟t be in dictionary.[8]

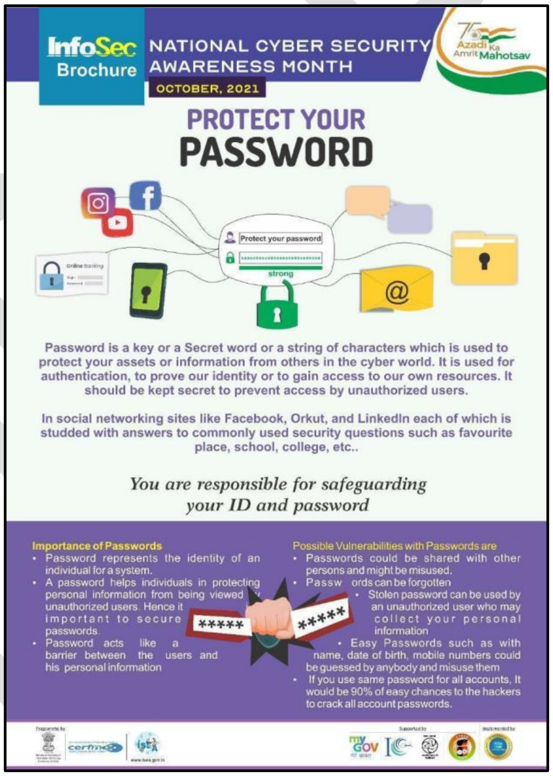
[8] Available at https://www.mha.gov.in/sites/default/files/Documents_InformationSecurity_25062019.pdf



गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS

Change your passwords regularly

Passwords should be changed at regular intervals as a precautionary measure



InfoSec Brochure

NATIONAL CYBER SECURITY AWARENESS MONTH

OCTOBER, 2021

Azadi Ka Amrit Mahotsav

PROTECT YOUR PASSWORD

Protect your password
strong
Online banking

Password is a key or a Secret word or a string of characters which is used to protect your assets or information from others in the cyber world. It is used for authentication, to prove our identity or to gain access to our own resources. It should be kept secret to prevent access by unauthorized users.

In social networking sites like Facebook, Orkut, and LinkedIn each of which is studded with answers to commonly used security questions such as favourite place, school, college, etc..

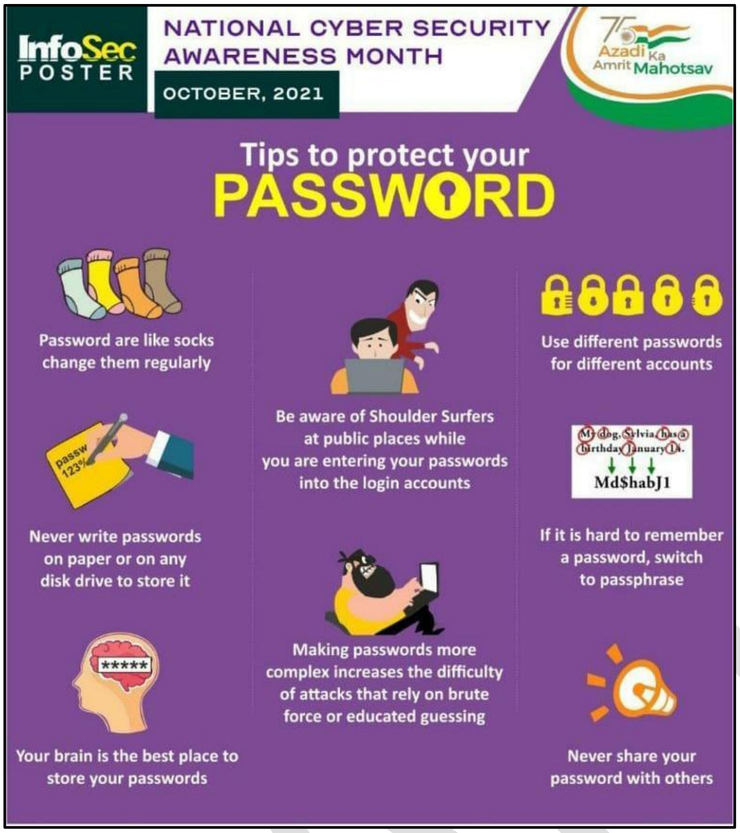
You are responsible for safeguarding your ID and password

Importance of Passwords

- Password represents the identity of an individual for a system.
- A password helps individuals in protecting personal information from being viewed by unauthorized users. Hence it important to secure passwords.
- Password acts like a barrier between the users and his personal information

Possible Vulnerabilities with Passwords are

- Passwords could be shared with other persons and might be misused.
- Passw ords can be forgotten
- Stolen password can be used by an unauthorized user who may collect your personal information
- Easy Passwords such as with name, date of birth, mobile numbers could be guessed by anybody and misuse them
- If you use same password for all accounts, It would be 90% of easy chances to the hackers to crack all account passwords.



InfoSec POSTER

NATIONAL CYBER SECURITY AWARENESS MONTH

OCTOBER, 2021

75 Azadi Ka Amrit Mahotsav

Tips to protect your PASSWORD

Password are like socks change them regularly

Be aware of Shoulder Surfers at public places while you are entering your passwords into the login accounts

Use different passwords for different accounts

Never write passwords on paper or on any disk drive to store it

My dog, Sylvia has a birthday January 1s.

Md$habJ1

If it is hard to remember a password, switch to passphrase

Making passwords more complex increases the difficulty of attacks that rely on brute force or educated guessing

Your brain is the best place to store your passwords

Never share your password with others

Incognito Mode

All major online browsers have a function that allows the user to open a private browsing window that deletes the browsing history when closed. It's known as Incognito Mode, Private Browsing, or InPrivate Browsing depending on the browser being used. Following are a few advantages of using private mode:

- **Deletes cookies:** Cookies are commonly used to provide a more targeted and customized browsing experience. Websites, on the other hand, can track these cookies and follow people around the web, compiling a thorough profile of their online behavior before sending them customized commercials. When a person logs out with Incognito Mode enabled, the browser will remove these cookies, keeping the personal settings hidden.

- **Keeps browsing history private:** If a person needs to check their email or shop online on a public computer, there's a good possibility the computer will save the browser history. This implies that the next person who logs on may be able to see all of the websites visited and even get into them using their credentials. Incognito Mode prevents this by removing any temporary browser data as soon as the person logs out.

- **Enables multiple sessions:** It allows people to login into multiple accounts at the same time. For example, a person may use an Incognito window to log into the work account while using a regular window to stay in their account.

TOOLS TO SAFEGUARD

Digi Locker

- The Government of India's Digi Locker is a cloud-based document storing solution.
- One of the main projects under the Digital India program is Digital Locker, which aims to eliminate the need for physical papers and facilitate the exchange of e-documents among government institutions via a process that verifies the documents' authenticity online.
- Users can also use the e-sign feature to submit their electronic documents and digitally sign them. These digitally signed papers can be shared with other government agencies or businesses.

Objectives of Digi Locker

- Enable digital empowerment of users by providing them with Digital Locker on the cloud.
- Enable e-Signing of documents and make them available electronically and online. Minimize the use of physical documents.
- Ensure the authenticity of the e-documents and thereby eliminate the usage of fake documents.
- Secure access to Govt. issued documents through a web portal and mobile application for residents.
- Reduce the administrative overhead of Govt. departments and agencies and make it easy for the users to receive services.
- Anytime, anywhere access to the documents by the user.

- Open and interoperable standards-based architecture to support a well-structured standard document format to support easy sharing of documents across departments and agencies.
- Ensure privacy and authorized access to users’ data.

Benefits of Digi Locker

- Users may exchange and view their digital papers from anywhere at any time. This is both practical and time-saving.
- It even cuts down on government agencies' administrative costs by reducing their reliance on paper.
- The most essential aspect is that because papers are issued directly by registered issuers, Digi Locker makes it easy to verify their validity.

How to use Digi Locker to keep originals

Step 1: To gain access to the digital locker, go on the official website, digitallocker.gov.in. Alternatively, the user can download the Digi Locker app on the device.

Step 2: After that, the user must click on Sign Up.

Step 3: On the following screen, enter the Aadhaar number.

Step 4: After the user has entered the 12-digit Aadhaar number, click Next. Two alternatives would be seen for moving forward: Use OTP or Use Fingerprint.

Step- 5: The user must first enter the Username and Password. The user can now enter the email address after selecting the chosen username and password for the Digital Locker account. If the user doesn't have one, simply select the Sign Up option.

Blockchain

A Blockchain is a digital, immutable, distributed ledger that records transactions in near real-time and tracks assets in a virtual network. An asset can be tangible (a house, car, cash, land) or intangible (intellectual property, branding). Virtually anything that has any value attached to it can be tracked and traded on a blockchain network. Each transaction is to be entered into the ledger, therefore providing a continual system of control regarding manipulation, mistakes, and data quality.

Blockchain, well known as the underlying technology driving Bitcoin, is one of the developing technologies that is now in use. Blockchain is a protocol that allows value to be exchanged over the internet without the necessity of a middleman.

Features Of a Blockchain

- **Near-real time:** Blockchain provides near-real-time settlement of recorded transactions, eliminating friction, and lowering risk.
- **No middleman:** Instead of faith, blockchain technology is based on cryptographic evidence allowing any two parties to interact directly with one other without the use of a middleman.
- **Distributed ledger:** A public history of transactions is kept by the peer-to-peer distributed network. The blockchain is made publicly available and widely accessible. Only the evidence of the transaction's existence is generally preserved by the blockchain, not the identities of the parties or the transaction data.
- **Irreversibility & Immutability:** The blockchain maintains a precise and verifiable record of every single transaction that has ever occurred. This prohibits previous blocks from being changed, therefore preventing duplicate spending, fraud, abuse, and transaction manipulation.
- **Smart Contracts:** Stored procedures that run on a Blockchain to perform predefined business processes and complete a commercially/legally enforceable transaction without the need for a middleman.

Parental Controls

Parental controls are features or software that allow parents to monitor and restrict what their child does online. There are a wide variety of programs that do such things as block and filter websites and content, record their activities, limit their time online, and view their browsing history and communications.

With ease of access, the internet exposes kids to various threats like identity theft, cyberbullying, social media scams, and malicious content. That is why parental control has become an essential requirement to protect kids.

M-Kavach

M-Kavach is a complete mobile device security solution for Android smartphones that addresses a variety of mobile phone risks. It defends against JavaScript Malware and handles dangers linked to the usage of resources such as WiFi, Bluetooth, Camera, and Mobile Data by blocking unauthorized access to these resources. Users may limit access to important apps such as mobile wallets and media apps, as well as prevent unsolicited calls and SMS. It also allows customers to follow SIM card changes on their smartphone in the event of device loss or theft, as well as erase contacts/call logs and factory reset the device remotely.

Features Of M-Kavach

- Access to essential apps is restricted.
- Access to Wi-Fi, Bluetooth, Camera, and Mobile Data is controlled by hardware.
- SMS notification of illegal SIM changes to a trustworthy cell phone number.
- Contacts and Call Logs may be remotely erased using the SMS Factory Reset option.
- Unwanted Calls & SMS are blocked when the device is reset remotely through SMS.
- Backups and restores are simple.
- Defends against JavaScript-based malware.

CHAPTER 5

Demystifying Institutional Framework of Cyber Security in India

National Cyber Security Centre

The National Cyber Security Centre (NCSC) was established in October 2016 with headquarters in London, bringing together expertise from CESG (GCHQ's information assurance arm), the Centre for Cyber Assessment, CERT-UK, and the Centre for Protection of National Infrastructure.

Ministry of Electronics and Information Technology (MeitY)

One of the most relevant objectives of MeitY is to handle e-security by securing India’s cyberspace. It plays an important role in preparing cyber laws, the administration of the Information Technology Act of 2000 (21 of 2000), and other IT-related legislation.

CERT-In
(Indian Computer Emergency Response Team)

Since January 2004, CERT-In has been in operation. The Indian Cyber Community is CERT-constituency. In's CERT-In is the federal entity in charge of responding to computer security incidents as they arise. CERT-In has been appointed as the national agency in charge of performing various cyber security functions.

The "Cyber Swachhta Kendra" (Botnet Cleaning and Malware Analysis Centre) is a part of the Indian Computer Emergency Response Team (CERT-In). It has been set up for analyzing BOTs/malware characteristics and providing information and enabling citizens for removal of BOTs/malware. In addition, "Cyber Swachhta Kendra" will strive to create awareness among citizens to secure their data, computers, mobile phones and devices such as home routers.

The National Cyber Coordination Centre (NCCC)

It is an operational cybersecurity and e-surveillance agency in India. It is jurisdictionally under the Ministry of Home Affairs. The NCCC coordinates with multiple security and surveillance agencies as well as with CERT-In of the Ministry of Electronics and Information Technology. Components of the NCCC include a cybercrime prevention strategy, cybercrime investigation training and review of outdated laws.

Centre for Development of Advanced Computing (CDAC)

The Ministry of Electronics and Information Technology's (MeitY) Centre for Development of Advanced Computing (C-DAC) is the ministry's primary research and development center for IT, electronics, and related fields. C-DAC has been conducting research and development in many sub-areas within the Cyber Security sector.

Information Security Education and Awareness (ISEA)

In 2014, MeitY approved a program named "Information Security Education and Awareness (ISEA) Phase II," which aims to build capacity in the area of information security by creating the right kind of qualified human resources to meet the ever-evolving challenges in this area through learning (formal and non-formal courses), training of government officials, and public awareness campaigns.

Cyber Surakshit Bharat Programme

Recognising the need to strengthen the cyber security ecosystem in India, and in alignment with the Honorable Prime Minister's vision for a 'Digital India,' the Ministry of Electronics and Information Technology (Meity), launched the Cyber Surakshit Bharat initiative in association with National e-Governance Division (NeGO) and industry partners. The purpose of the program is to spread awareness, build capacity as well as enable government departments on steps that need to be taken to create a resilient IT set up.

National Critical Information Infrastructure Protection Centre (NCIIPC)

The National Critical Information Infrastructure Protection Centre (NCIIPC) is a government of India entity that was established under Sec 70A of the Information Technology Act, 2000 (as amended 2008). In terms of Critical Information Infrastructure Protection, it has been designated as the National Nodal Agency. The goal is to provide a safe, secure, and reliable information infrastructure for the nation's critical sectors.

Ministry of Home Affairs (MHA)

Cyber And Information Security (C&Is) Division

The division is responsible for Cyber Security, Cyber Crime, the National Information Security Policy and Guidelines (NISPG), and the implementation of NISPG, NATGRID, and other related issues.

Indian Cyber Crime Coordination Center

The government recently launched the Indian Cyber Crime Coordination Centre (I4C). In addition, the National Cyber Crime Reporting Portal has been launched across India. In October 2018, the plan to establish I4C was authorized, to deal with all sorts of cybercrime in a comprehensive and coordinated manner.

@CyberDost

The Ministry of Home Affairs started the @CyberDost Twitter handle in 2018 intending to raise awareness about cybercrime and the necessary safeguards to be taken. All the citizens and government officials must follow this Twitter handle to be greatly benefited. This will improve their basic understanding of cybercrime and the actions that should be taken to avoid it.

Cybercrime Prevention Against Women And Children (CCPWC) Scheme

Under the scheme:

- States/UTs have been given an INR 87.12 crore grant to set up Cyber Forensic Training Labs and hire Jr Cyber Forensic Consultants to run the labs in their respective states.
- States/UTs have been given INR 6 crore in funding to train 40500 police, prosecutors, and judicial officers by 31-3-2020.
- For tweets about cybercrime awareness, the Twitter handle "CyberDost" was created.
- Proposals have been received for the establishment of a Cyber Crime Prevention and Control Centre of Excellence for R&D.
- NEPA offered a five-day course on "Cybercrime Investigation" for twenty-three police personnel from Meghalaya from April 2 to 6, 2018.

State Cyber Cells

The Delhi Police's CyPAD (Cyber Prevention & Awareness Detection) unit is part of the Special Cell. The Delhi Police's Cyber Crime Cell is a specialized division that investigates all complex and sensitive cyber incidents, particularly those involving women and children as victims. The Cyber Crime Cell has a Cyber Lab with cyber forensic capabilities such as data extraction from hard drives and mobile phones, imaging and hash value calculation, forensic servers, and portable forensic tools for the on-site examination.

CHAPTER 6

Glimpses into the Legal Framework for Cyber Security and Privacy in India

IT ACT 2000 / ITAA 2008

New types of cybercrime have emerged as a result of the rapid growth in the usage of computer systems and internet users, for which the Central Government has made frequent amendments. The following are some key provisions to consider:

Relevant IT Act Sections:

- Section 43 – Penalty and Compensation for damage to a computer, computer system, etc.
- Section 65 – Tampering with Computer Source Documents
- Section 66A – Punishment for sending offensive messages through communication service

Relevant Case - Bomb Hoax mail:

In 2009, a 15-year-old Bangalore teenager was arrested by the cybercrime investigation cell (CCIC) of the city crime branch for allegedly sending a hoax email to a private news channel. In the email, he claimed to have planted five bombs in Mumbai, challenging the police to find them before it was too late. At around 1 p.m. on May 25th, the news channel received an email that read: "I have planted five bombs in Mumbai; you have two hours to find it." The police, who were alerted immediately, traced the Internet Protocol (IP) address to Vijay Nagar in Bangalore.
The Internet service provider for the account was BSNL, said officials.

- Section – 66F Cyber Terrorism:
- Section 66C – Punishment for identity theft
- Section 66D – Punishment for cheating by impersonation using computer resources
- Section 67 – Punishment for publishing or transmitting obscene material in electronic form

Relevant Case:

This case is about posting obscene, defamatory, and annoying messages about a divorced woman in the Yahoo message group. Emails were forwarded to the victim for information by the accused through a false e-mail account opened by him in the name of the victim. These postings resulted in annoying phone calls to the lady. Based on the lady’s complaint, the police nabbed the accused. Investigations revealed that he was a known family friend of the victim and was interested in marrying her. She was married to another person, but that marriage ended in divorce and the accused started contacting her once again. On her reluctance to marry him he started harassing her through the internet.

Verdict: The accused was found guilty of offenses under sections 469, 509 IPC, and 67 of IT Act 2000. He is convicted and sentenced for the offense as follows: As per 469 of IPC, he must undergo rigorous imprisonment for 2 years and must pay a fine of Rs.500/-. As per 509 of IPC, he is to undergo 1-year simple imprisonment and to pay Rs 500/-. As per Section 67 of IT Act 2000, he must undergo for 2 years and to pay a fine of Rs.4000/-. All sentences were to run concurrently. The accused paid the fine amount, and he was lodged at Central Prison, Chennai. This is considered the first case convicted under section 67 of the Information Technology Act 2000 in India.

- Section 66E – Punishment for violation of privacy

Relevant Cases:

Jawaharlal Nehru University MMS scandal - In a severe shock to the prestigious and renowned institute, Jawaharlal Nehru University, a pornographic MMS clip was made on the campus and transmitted outside the university. Some media reports claimed that the two accused students initially tried to extort money from the girl in the video but when they failed the culprits put the video out on cell phones, on the internet, and even sold it as a CD in the blue film market.

- Section 69 – Powers to issue directions for interception or monitoring or decryption of any information through any computer resource

Indian Penal Code (IPC), 1860

The Indian Penal Code codifies criminal offenses and guides cybercrime as well. The acts covered by the Information Technology Act of 2000 are based on the offenses codified under the Indian Penal Code (IPC), 1860, which are related to computer and internet use. To make the punishment severe for the offender, Legal Enforcement Agencies use parts of the Indian Penal Code (IPC) from 1860 as well as the Information Technology Act of 2000.

National Cyber Security Policy, 2013

The purpose of this policy document is to ensure secure cyberspace for citizens, businesses, and the government. As per Cyber security guidelines (ISO/IEC 27032-2012) ‘Cyberspace’ is a complex environment consisting of interactions between people, software, and services supported by the worldwide distribution of information and communication technology (ICT) devices and networks.

With the growth of the IT sector in the country, ambitious plans for rapid social transformation and inclusive growth, and the prominent role of India in the IT global market, a national policy was much needed for creating a secure computing environment for building adequate trust and confidence in information flow, public service delivery and electronic transactions occurring via cyberspace.

The National Cyber Security Policy was formulated by the Ministry of Electronics and Information Technology (MeitY), Government of India in 2013. The policy is aimed at building secure and resilient cyberspace for citizens, businesses, and governments**.**

It also enables the individual sectors and organizations in designing appropriate cyber security policies to suit their needs. The mission of the policy is to protect information and information infrastructure in cyberspace, build capabilities to prevent and respond to cyber threats, reduce vulnerabilities and minimize damage from cyber incidents through a combination of institutional structures, people, processes, technology, and cooperation.

CHAPTER 7

What To Do If A Victim Of A CyberCrime

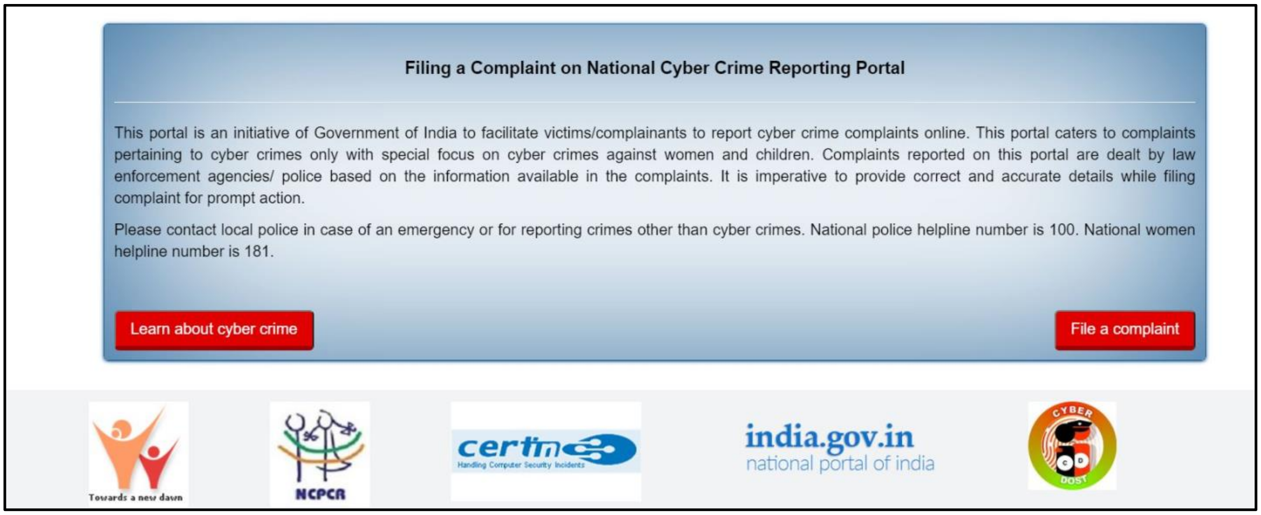
How and Where To Lodge a Cyber Crime Complaint

- Open the website –**https://cybercrime.gov.in/**

Step 1 - After opening the website, the person will see a prompt on the screen. One can notice, next to the home button tab, there are two other options – Report Women/Child-Related Crime and Report Other Cyber Crime.

Step 2 - If a woman or a child is a victim of cybercrime, then click this button. Upon clicking, the person will find an option of Report anonymously and report & track. If one wants to hide the identity, then the anonymous option can be chosen, else the report and track button should be pressed.

Step 3: In the next window, users have to press – File a complaint and I Accept button to move forward. One must read the conditions and accept. The portal states — Please contact local police in case of an emergency or for reporting crimes other than cybercrimes. The national police helpline number is 112. The national women helpline number is 181.

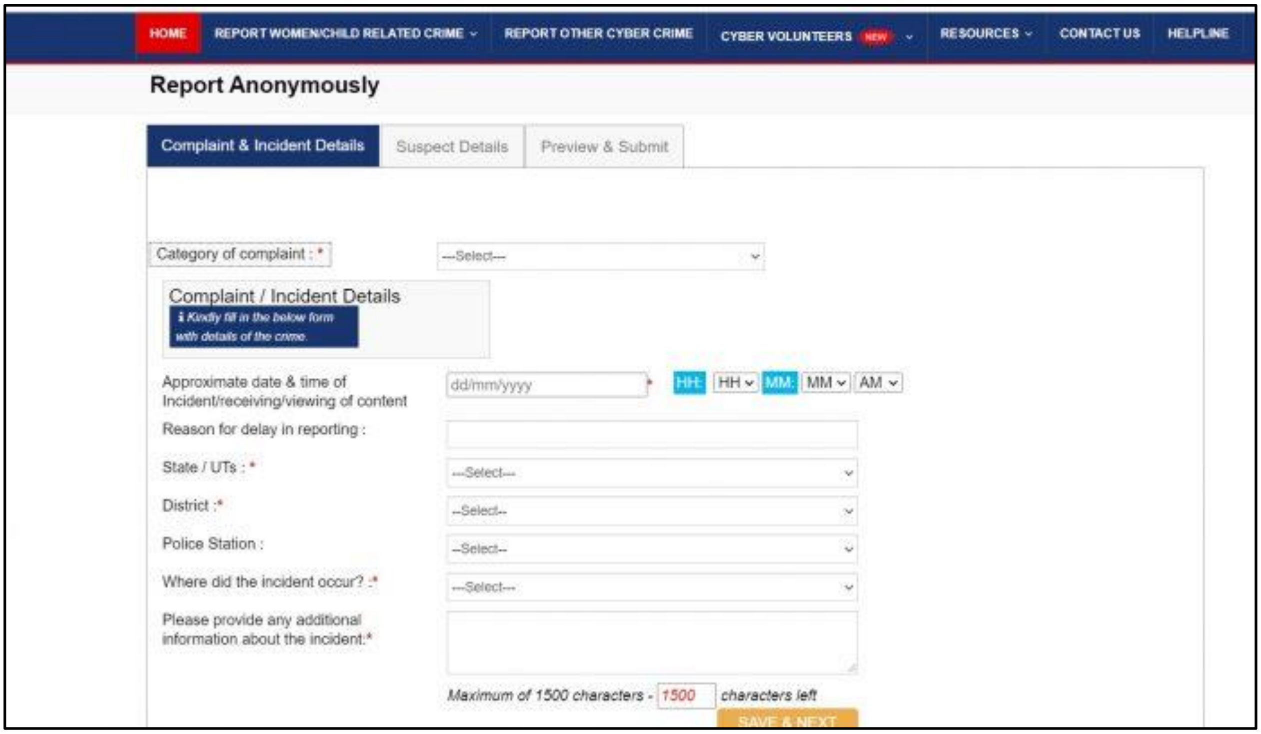


Filing a Complaint on National Cyber Crime Reporting Portal

This portal is an initiative of Government of India to facilitate victims/complainants to report cyber crime complaints online. This portal caters to complaints pertaining to cyber crimes only with special focus on cyber crimes against women and children. Complaints reported on this portal are dealt by law enforcement agencies/ police based on the information available in the complaints. It is imperative to provide correct and accurate details while filing complaint for prompt action.

Please contact local police in case of an emergency or for reporting crimes other than cyber crimes. National police helpline number is 100. National women helpline number is 181.

Step 4: Here, the user creates a user id and registers the mobile number on which they will receive OTP, and fill in the name and state columns. After successfully logging in to the page, one can easily choose the respective area and register a complaint. Fill in the relevant details about the offense.



Report Anonymously

Category of complaint : * ---Select---

Complaint / Incident Details

Kindly fill in the below form with details of the crime.

Approximate date & time of Incident/receiving/viewing of content: dd/mm/yyyy HH: HH MM: MM AM

Reason for delay in reporting :

State / UTs : * ---Select---

District :* --Select--

Police Station : --Select--

Where did the incident occur? :* ---Select---

Please provide any additional information about the incident:*

Maximum of 1500 characters - 1500 characters left

Follow similar steps to file a complaint under the “report other cybercrimes” option. Select the appropriate category and sub-category.

Tracking the complaint

Once the person has registered the complaint on the website, they will receive a unique number for reference. Further communication regarding the investigations will be done via a unique number generated. The number can also be used to track the status of the complaint.

Registering complaint via an email

One can also send a mail to complaint-mwcd@gov.in, a hotline created by the Ministry of Women and Child development to report online bullying and abuse.

There is also a facility for getting the investigation done without getting identity disclosed. There are Cyber Nodal Officers designated in almost every corner of the country.

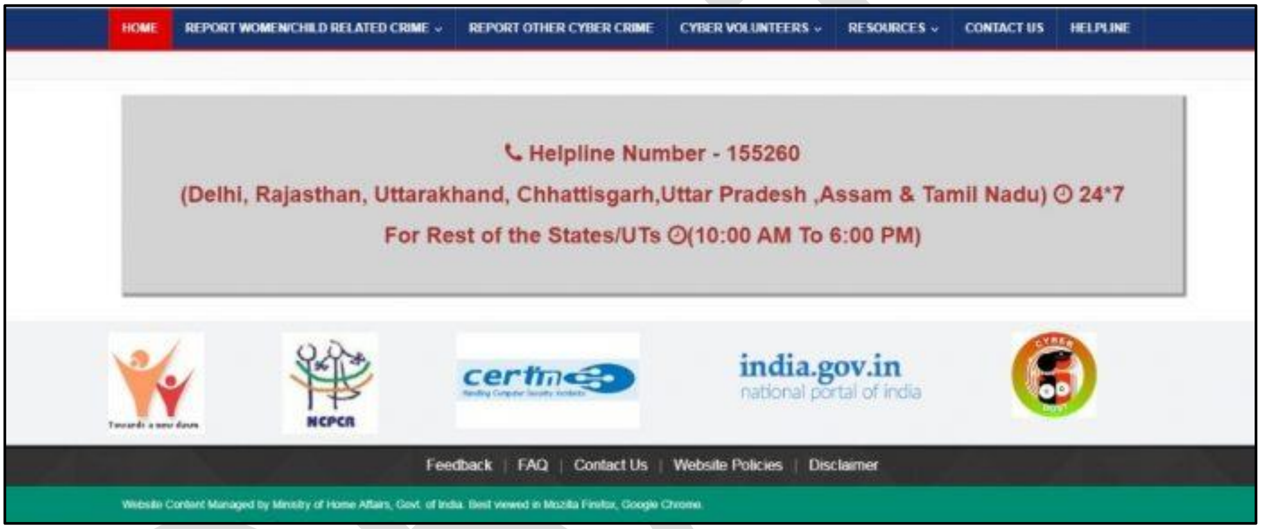
A complaint can be registered by emailing security officers on their respective email id. Full List here: https://cybercrime.gov.in/Webform/Crime_NodalGrivanceList.aspx

A PDF file with the list of email id and contact numbers of the nodal officers is available in the Contact Us section on the cybercrime.gov.in website.

Helpline numbers and Portals

Helpline number for reporting cybercrime: 1930

Portal to lodge a complaint: cybercrime.gov.in



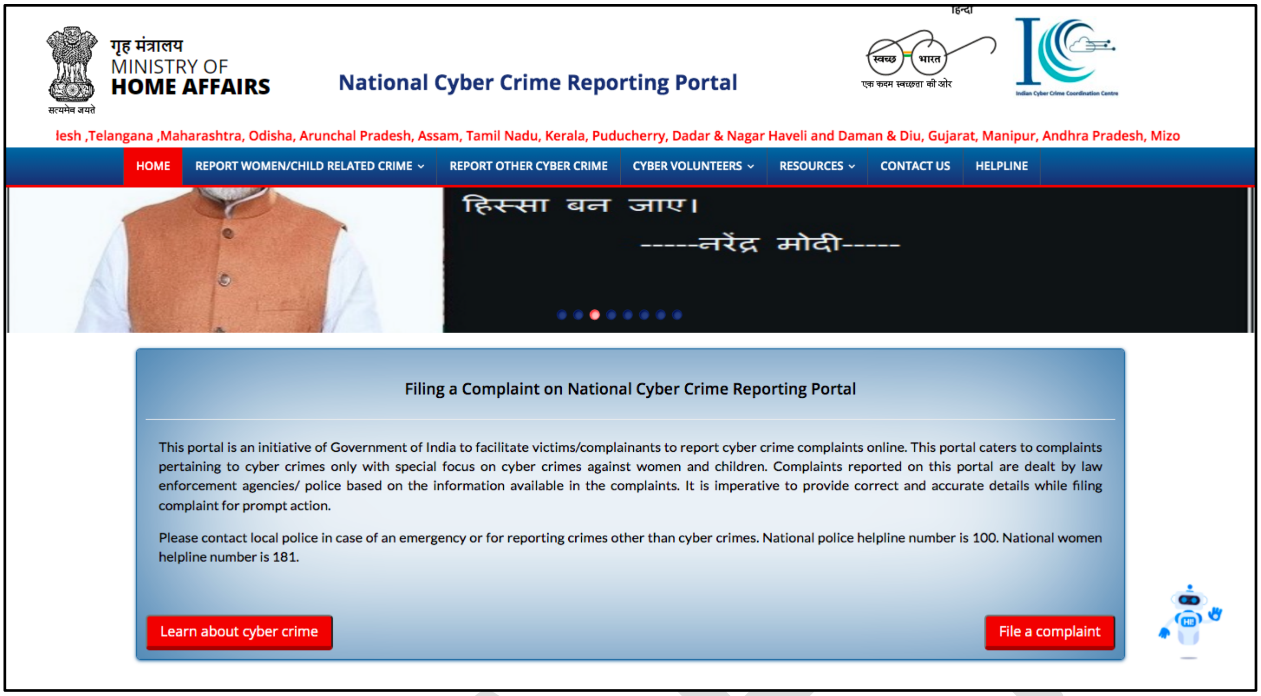
☎ Helpline Number - 155260

(Delhi, Rajasthan, Uttarakhand, Chhattisgarh,Uttar Pradesh ,Assam & Tamil Nadu) 24*7

For Rest of the States/UTs (10:00 AM To 6:00 PM)

Website Content Managed by Ministry of Home Affairs, Govt. of India. Best viewed in Mozilla Firefox, Google Chrome.

National Cyber Crime Reporting Portal


गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS
सत्यमेव जयते
National Cyber Crime Reporting Portal
हिन्दी
स्वच्छ भारत
एक कदम स्वच्छता की ओर
Indian Cyber Crime Coordination Centre
lesh ,Telangana ,Maharashtra, Odisha, Arunchal Pradesh, Assam, Tamil Nadu, Kerala, Puducherry, Dadar & Nagar Haveli and Daman & Diu, Gujarat, Manipur, Andhra Pradesh, Mizo
HOME
REPORT WOMEN/CHILD RELATED CRIME
REPORT OTHER CYBER CRIME
CYBER VOLUNTEERS
RESOURCES
CONTACT US
HELPLINE
हिस्सा बन जाए।
-----नरेंद्र मोदी-----
Learn about cyber crime
File a complaint
HI

Filing a Complaint on National Cyber Crime Reporting Portal

This portal is an initiative of Government of India to facilitate victims/complainants to report cyber crime complaints online. This portal caters to complaints pertaining to cyber crimes only with special focus on cyber crimes against women and children. Complaints reported on this portal are dealt by law enforcement agencies/ police based on the information available in the complaints. It is imperative to provide correct and accurate details while filing complaint for prompt action.

Please contact local police in case of an emergency or for reporting crimes other than cyber crimes. National police helpline number is 100. National women helpline number is 181.

- It is a citizen-centric initiative that was launched in 2019 that allows citizens to report cybercrime online.
- The portal focuses on crimes against women and children, including child pornography, child sex abuse material, and online content related to rapes/gang rapes, among other things.
- It also focuses on financial crimes and crimes involving social media, such as stalking and cyberbullying.
- It will strengthen law enforcement agencies' capacity to investigate cases after they have been completed successfully by improving coordination between law enforcement agencies from different states, districts, and police stations.
- In the case of an emergency or to report crimes other than cybercrime, contact the local police department. The number for the national police helpline is 100.

Helplines and Portals (Women and Children)

- Women

□ Helpline number: 1091, 181

□ Portal to lodge complaint by National Commission for Women: ncw.nic.in

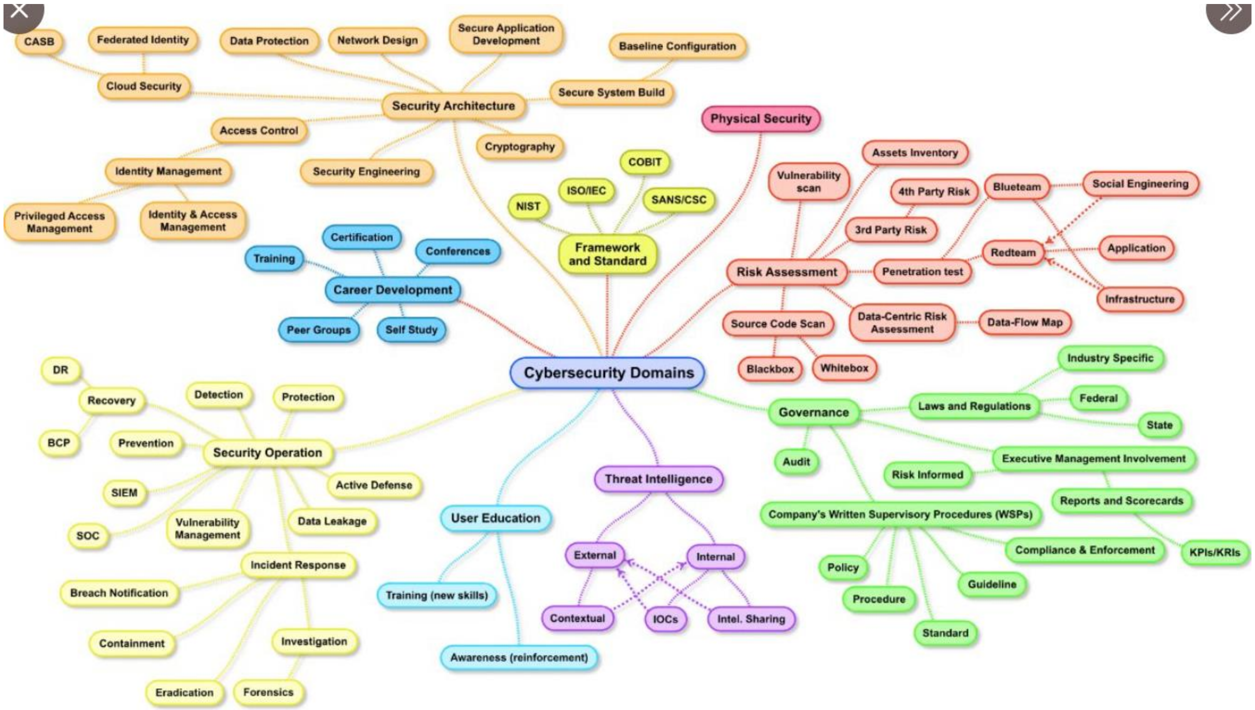
- Children
  - Helpline number: 1098
  - Helpline number by DCPCR (Delhi Commission for Protection of Child Rights) : +91-9311551393

Reporting International Fraud Calls:
DoT Tollfree: 1800110420/ 1963

CHAPTER 8

Strengthening Students

Career Opportunities



Job Profiles

- Cybercrime Investigator
- Intelligence Analyst
- Consultant
- Cyber Forensics Expert
- IT Security Risk and Compliance Analyst
- Cyber Security Researchers
- Technology Analyst
- Cyber Security Instructor

Universities

Bachelors' Programmes

- B.E in cyber security (SRM Valliammai Engineering College, Kancheepuram)
- B.Tech. in Computer Science and Engineering (Cyber security) (HITAM Hyderabad)
- B.Sc. in cyber security (K.R. Mangalam University (Gurgaon), NIMAS (Kolkata))
- B.Tech CSE-Networking and cyber security (Sharda University, Greater Noida)

Masters' Programmes

- M.Sc. in Cyber Security/M.Tech in cyber security (Calicut University)
- M.Sc. in Advanced Networking and Cyber Security (Brainware University)
- M.Sc. in Information and Cyber Security (NSHM Knowledge Campus(Kolkata), Amity University (Jaipur), Webel Fujisoft Vara Centre of Excellence (Kolkata), Marwadi University (Rajkot))
- M.Sc. in Advanced Networking and Cyber Security (Swami Vivekananda University (SVU), Kolkata)
- M.Tech CSE-Networking and cyber security (Sharda University, Greater Noida)
- M.Tech CSE – Cyber Forensics and Information Security (ERDC Institute of Technology, Thiruvananthapuram)

Diploma Programmes

- PG Diploma in Information Security and Cloud Computing-certificate in information security (NIELIT Delhi)
- Diploma in Cyber Security (HITS Chennai)

Certifications and Other

The CCISO certificate is the highest achievement offered to chief information security officers. OSCP (Offensive Security Certified Professional), SANS Technology Institute, ISFCE (International Society of Forensic Computer Examiners), IACIS (The International Association of Computer Investigative Specialists), GIAC (Global Information Assurance Certification), CISSP (Certified Information Systems Security Professional), and (ISC)2 (International Information Systems Security Certification) are among the organization unauthorized that provide training and certifications.

MOOC (NCTC)

- Common Cyber Crime Course
- Cybercrime Awareness for Police Officers
- Cybercrime Investigation: Case Studies
- Cybercrime Investigation: Hands-on Approach
- Fingerprint Course
- Judiciary / Prosecution Track
- Investigation Track

CHAPTER 9

Strengthening Educational Setups

Tool Kits Available

CCMP

For combating cyber attacks, the government has developed a **Cyber Crisis Management Plan** (CCMP), which will be implemented by all Central Government Ministries/Departments, State Governments and their entities, and critical sectors.

Other related sources available

- Child Victims of Cyber Crime Legal Toolkit

https://ncpcr.gov.in/showfile.php?lang=1&level=1&&sublinkid=1298&lid=1519

- ITU Toolkit for Cyber Crime Legislation

https://www.combattingcybercrime.org/files/virtual-library/assessment-tool/itu-toolkit-for-cybercrime-legislation-%28draft%29.pdf

Suggested Cyber Policy Guidelines for HEIs

Policies that clearly define what should be done and what should not be done while executing specific tasks can help minimize the risk of cyber threats. Various federal rules require IHEs to guarantee the privacy, security, and confidentiality of personally identifiable information (PII) and/or information security. These include the following:

- The Family Educational Rights and Privacy Act (FERPA) prohibits educational institutions from revealing student PII or education information without written consent.
- The Federal Information Security Modernization Act of 2014 (FISMA 2014) mandates the security of federal data.
- The Gramm-Leach-Bliley Act (GLBA) requires financial institutions, including colleges and universities, to protect customer personal information (PII).

- The Health Insurance Portability and Accountability Act (HIPAA) requires institutions to secure health records and other identifiable health information by implementing privacy safeguards and prohibiting unauthorized uses and disclosures.
- Higher Education Act (HEA) requires IHEs with Title IV programs to have information security policies, controls, monitoring, and management procedures.
- Enrollment Agreement with the Student Aid Internet Gateway (SAIG) requires IHEs with Title IV programs to preserve all Federal Student Aid applicant information.

When developing cybersecurity plans, policies, and procedures for use by staff (IT, emergency management, academic, research, administrative, and other), students, and visitors, IHEs must keep these Federal regulations in mind, as well as state and local laws related to managing information security in the academic setting.

NISPG Guidelines by MHA

The Ministry of Home Affairs (MHA) has been given the task of coordinating and managing public and private sector information security activities. It developed a National Information Security Policy and Guidelines (NISPG), established information handling processes, and provided security guidelines for classified information assets.

The policy proposes that each government organization establish a security division responsible for planning, implementing, and overseeing all activities related to information security in a comprehensive and focused manner. The security division will be responsible for risk analysis based on threat and risk assessments emerging from technology adoption.

Eight domains are critical for implementing a good information security program as they handle the specifics that have been crucial to its performance. Each domain's contribution to the information security program's success is linked with the maturity and success of the other domains. As a result, they work together to establish a foundation for a strong information security program. These domains are:

- Network and Infrastructure security
- Identity, access, and privilege management
- Physical security
- Application security
- Data security
- Personnel security
- Threat and vulnerability management
- Security and incident management

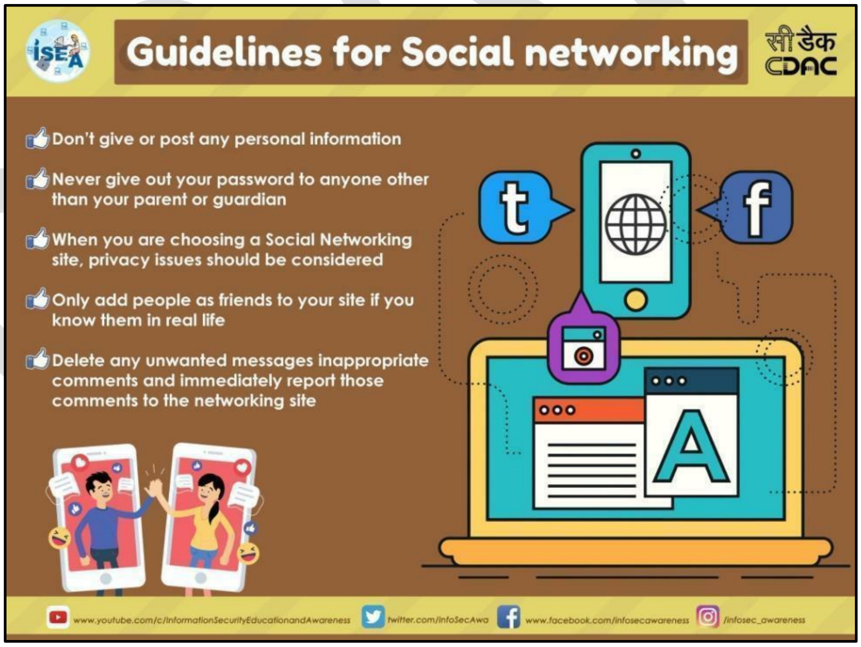
CHAPTER 10

Strengthening Teachers & IT Teams of HEIs

Some Existing Training Initiatives - CISO training

The Certified CISO (CCISO) program is a unique training module in terms of providing training and certification for information security executives at the highest levels. The CCISO focuses on the application of information security management principles from an executive management perspective, rather than on technical competence. For present and aspiring CISOs, the program was created by sitting CISOs. The Chief Information Security Officer Certification Training covers policy development, project management, audit management, executive strategy, contract management, and financial competence.

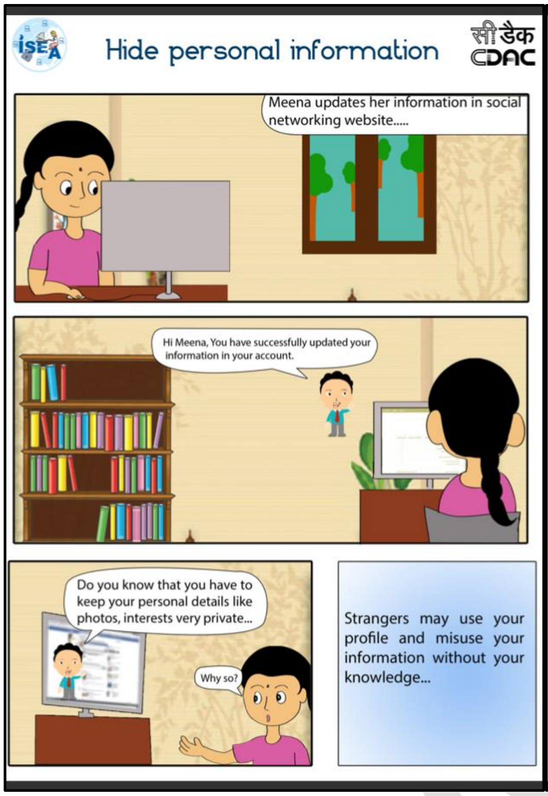
Design Reference Samples:



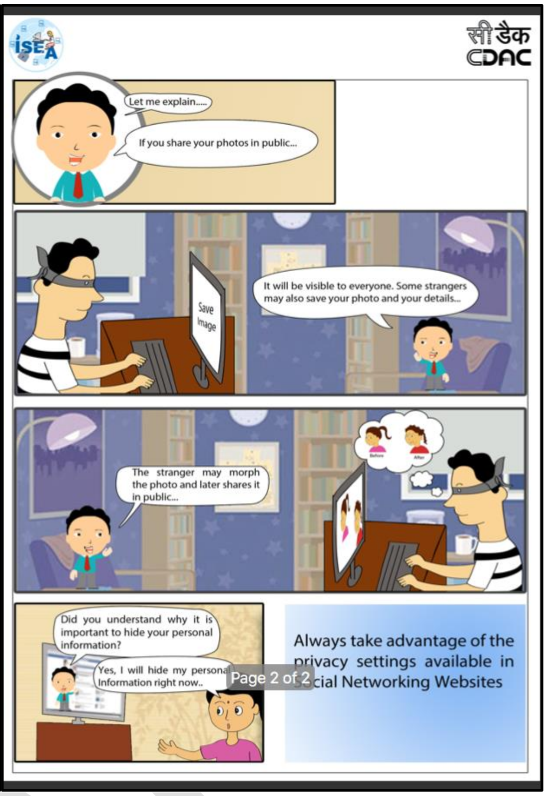
Guidelines for Social networking

- Don't give or post any personal information
- Never give out your password to anyone other than your parent or guardian
- When you are choosing a Social Networking site, privacy issues should be considered
- Only add people as friends to your site if you know them in real life
- Delete any unwanted messages inappropriate comments and immediately report those comments to the networking site

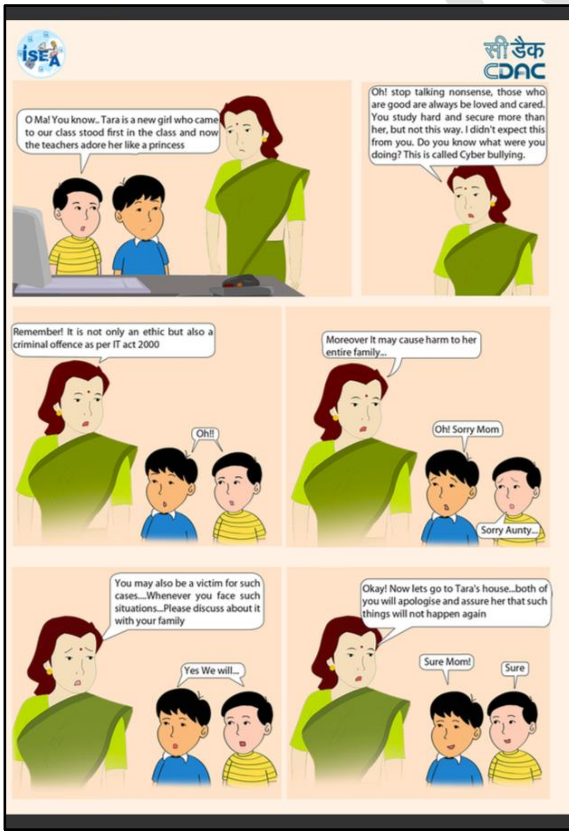
www.youtube.com/c/InformationSecurityEducationandAwareness twitter.com/InfoSecAwa www.facebook.com/infosecawareness /infosec_awareness

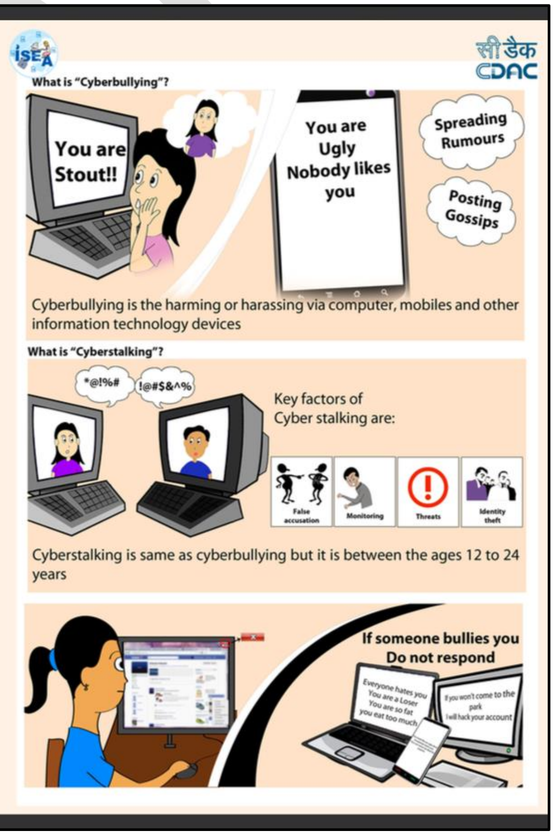

ISEA
सी डैक CDAC
Hide personal information
Meena updates her information in social networking website.....
Hi Meena, You have successfully updated your information in your account.
Do you know that you have to keep your personal details like photos, interests very private...
Why so?

Strangers may use your profile and misuse your information without your knowledge...


ISEA
सी डैक CDAC
Let me explain.....
If you share your photos in public...
Save Image
It will be visible to everyone. Some strangers may also save your photo and your details...
The stranger may morph the photo and later shares it in public...
Before
After
Did you understand why it is important to hide your personal information?
Yes, I will hide my personal Information right now..
Page 2 of 2

Always take advantage of the privacy settings available in Social Networking Websites


ISEA
सी डैक CDAC
O Ma! You know.. Tara is a new girl who came to our class stood first in the class and now the teachers adore her like a princess
Oh! stop talking nonsense, those who are good are always be loved and cared. You study hard and secure more than her, but not this way. I didn't expect this from you. Do you know what were you doing? This is called Cyber bullying.
Remember! It is not only an ethic but also a criminal offence as per IT act 2000
Oh!!
Moreover It may cause harm to her entire family...
Oh! Sorry Mom
Sorry Aunty...
You may also be a victim for such cases....Whenever you face such situations...Please discuss about it with your family
Yes We will...
Okay! Now lets go to Tara's house...both of you will apologise and assure her that such things will not happen again
Sure Mom!
Sure


ISEA
सी डैक CDAC
You are Stout!!
You are Ugly Nobody likes you
Spreading Rumours
Posting Gossips
*@!%#
!@#$&^%
False accusation
Monitoring
Threats
Identity theft
Everyone hates you You are a Loser You are so fat you eat too much
If you won't come to the park I will hack your account

What is "Cyberbullying"?

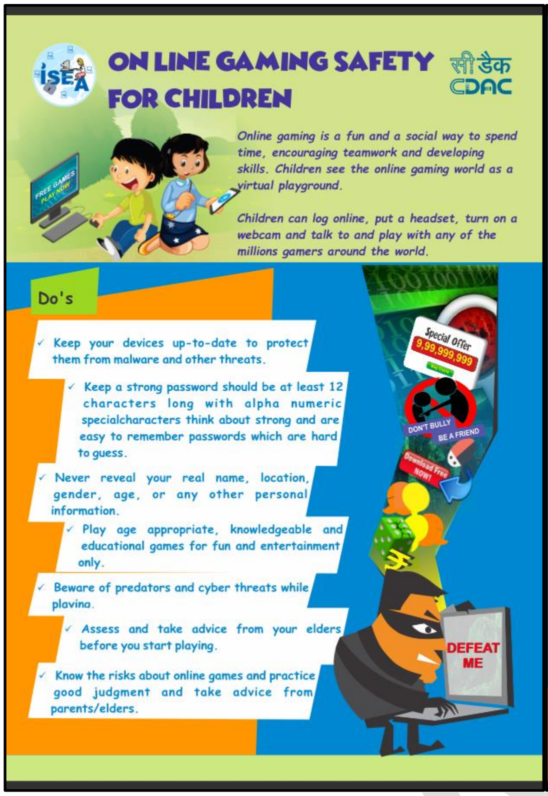
Cyberbullying is the harming or harassing via computer, mobiles and other information technology devices

What is "Cyberstalking"?

Key factors of Cyber stalking are:

Cyberstalking is same as cyberbullying but it is between the ages 12 to 24 years

If someone bullies you Do not respond



ISEA सी डैक CDAC

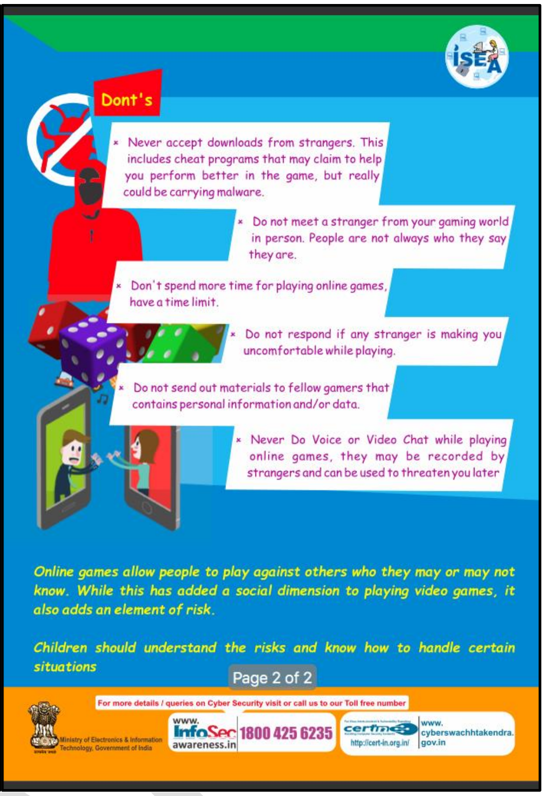
ON LINE GAMING SAFETY FOR CHILDREN

Online gaming is a fun and a social way to spend time, encouraging teamwork and developing skills. Children see the online gaming world as a virtual playground.

Children can log online, put a headset, turn on a webcam and talk to and play with any of the millions gamers around the world.

Do's

- ✓ Keep your devices up-to-date to protect them from malware and other threats.
- ✓ Keep a strong password should be at least 12 characters long with alpha numeric specialcharacters think about strong and are easy to remember passwords which are hard to guess.
- ✓ Never reveal your real name, location, gender, age, or any other personal information.
- ✓ Play age appropriate, knowledgeable and educational games for fun and entertainment only.
- ✓ Beware of predators and cyber threats while plavina.
- ✓ Assess and take advice from your elders before you start playing.
- ✓ Know the risks about online games and practice good judgment and take advice from parents/elders.



ISEA

Dont's

- × Never accept downloads from strangers. This includes cheat programs that may claim to help you perform better in the game, but really could be carrying malware.
- × Do not meet a stranger from your gaming world in person. People are not always who they say they are.
- × Don't spend more time for playing online games, have a time limit.
- × Do not respond if any stranger is making you uncomfortable while playing.
- × Do not send out materials to fellow gamers that contains personal information and/or data.
- × Never Do Voice or Video Chat while playing online games, they may be recorded by strangers and can be used to threaten you later

Online games allow people to play against others who they may or may not know. While this has added a social dimension to playing video games, it also adds an element of risk.

Children should understand the risks and know how to handle certain situations

Page 2 of 2

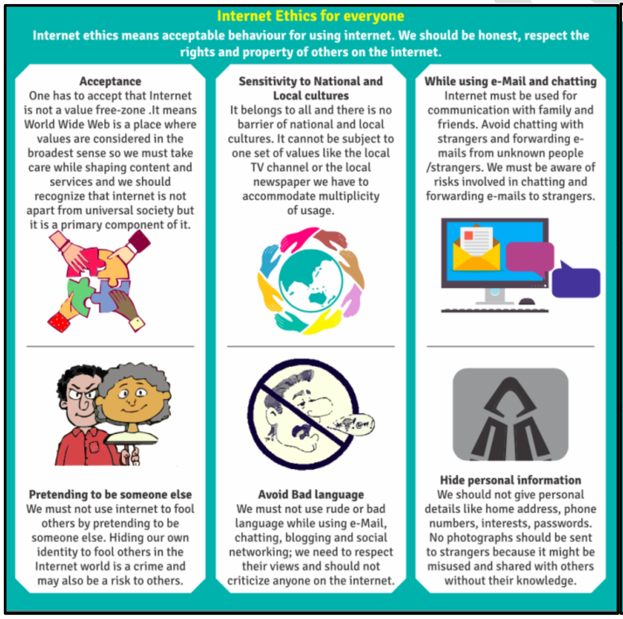
For more details / queries on Cyber Security visit or call us to our Toll free number

Ministry of Electronics & Information Technology, Government of India

www.InfoSec awareness.in 1800 425 6235

cert-in http://cert-in.org.in/

www.cyberswachhtakendra.gov.in



Internet Ethics for everyone

Internet ethics means acceptable behaviour for using internet. We should be honest, respect the rights and property of others on the internet.

Acceptance
One has to accept that Internet is not a value free-zone .It means World Wide Web is a place where values are considered in the broadest sense so we must take care while shaping content and services and we should recognize that internet is not apart from universal society but it is a primary component of it.

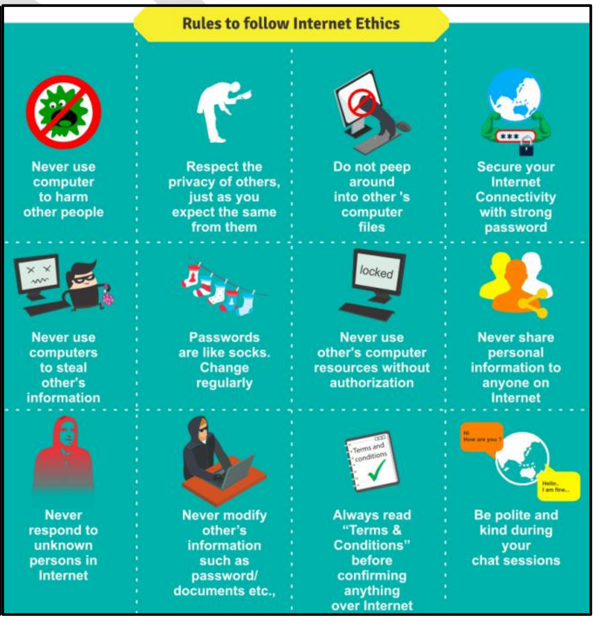
Sensitivity to National and Local cultures
It belongs to all and there is no barrier of national and local cultures. It cannot be subject to one set of values like the local TV channel or the local newspaper we have to accommodate multiplicity of usage.

While using e-Mail and chatting
Internet must be used for communication with family and friends. Avoid chatting with strangers and forwarding e-mails from unknown people /strangers. We must be aware of risks involved in chatting and forwarding e-mails to strangers.

Pretending to be someone else
We must not use internet to fool others by pretending to be someone else. Hiding our own identity to fool others in the Internet world is a crime and may also be a risk to others.

Avoid Bad language
We must not use rude or bad language while using e-Mail, chatting, blogging and social networking; we need to respect their views and should not criticize anyone on the internet.

Hide personal information
We should not give personal details like home address, phone numbers, interests, passwords. No photographs should be sent to strangers because it might be misused and shared with others without their knowledge.



Rules to follow Internet Ethics

Never use computer to harm other people

Respect the privacy of others, just as you expect the same from them

Do not peep around into other 's computer files

Secure your Internet Connectivity with strong password

Never use computers to steal other's information

Passwords are like socks. Change regularly

Never use other's computer resources without authorization

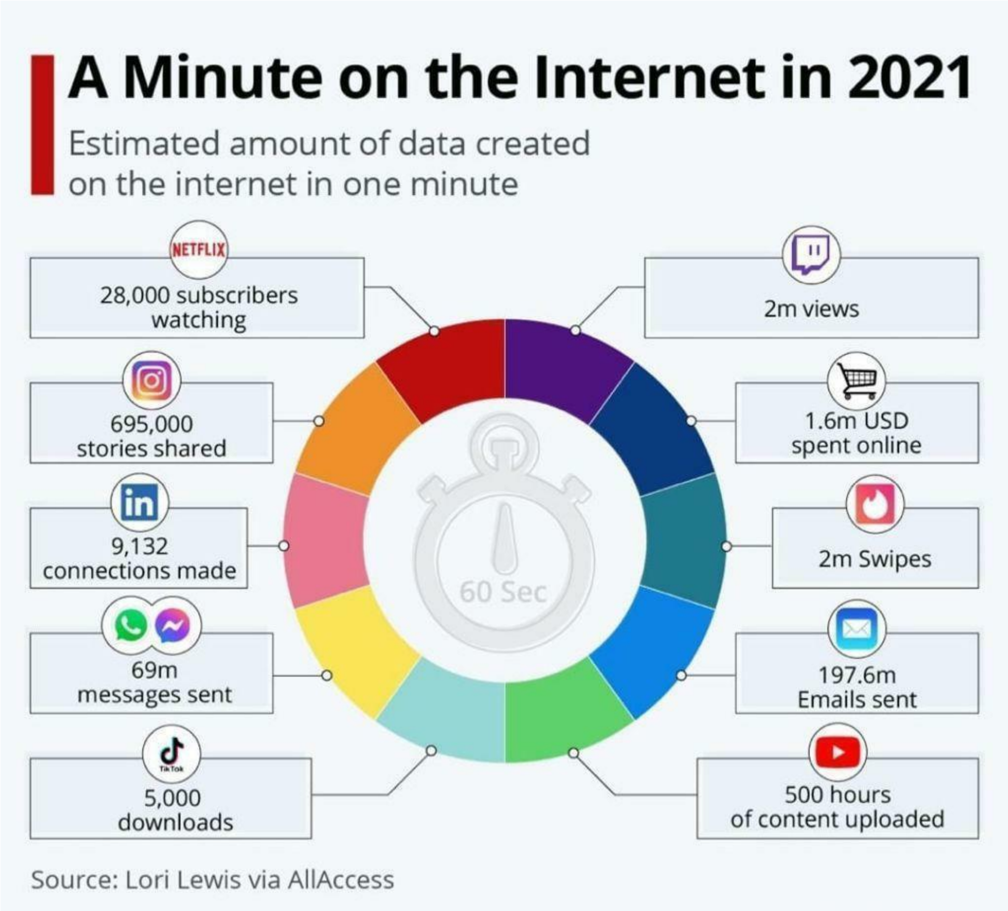
Never share personal information to anyone on Internet

Never respond to unknown persons in Internet

Never modify other's information such as password/ documents etc.,

Always read "Terms & Conditions" before confirming anything over Internet

Be polite and kind during your chat sessions

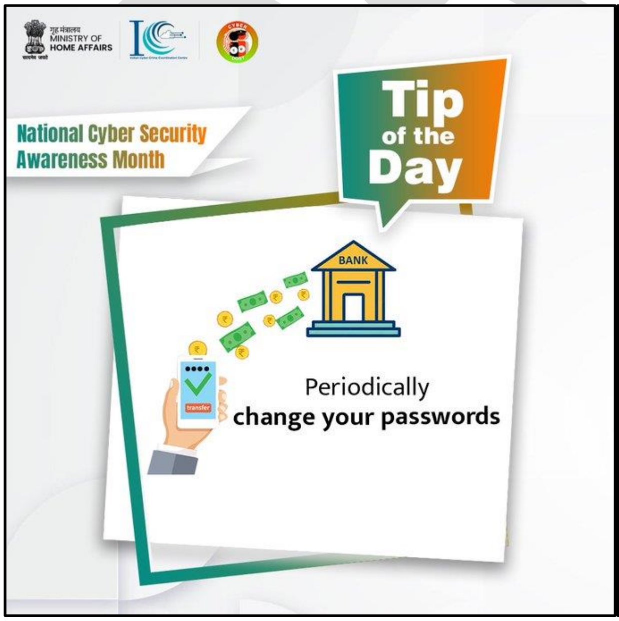


A Minute on the Internet in 2021

Estimated amount of data created on the internet in one minute

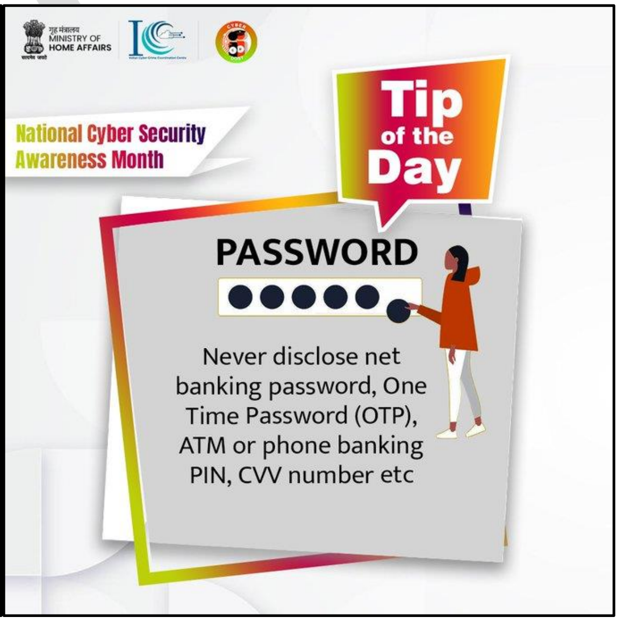
- 28,000 subscribers watching
- 695,000 stories shared
- 9,132 connections made
- 69m messages sent
- 5,000 downloads
- 2m views
- 1.6m USD spent online
- 2m Swipes
- 197.6m Emails sent
- 500 hours of content uploaded

Source: Lori Lewis via AllAccess



National Cyber Security Awareness Month

Periodically **change your passwords**



National Cyber Security Awareness Month

Never disclose net banking password, One Time Password (OTP), ATM or phone banking PIN, CVV number etc

गृह मंत्रालय MINISTRY OF HOME AFFAIRS

National Cyber Security Awareness Month

Tip of the Day

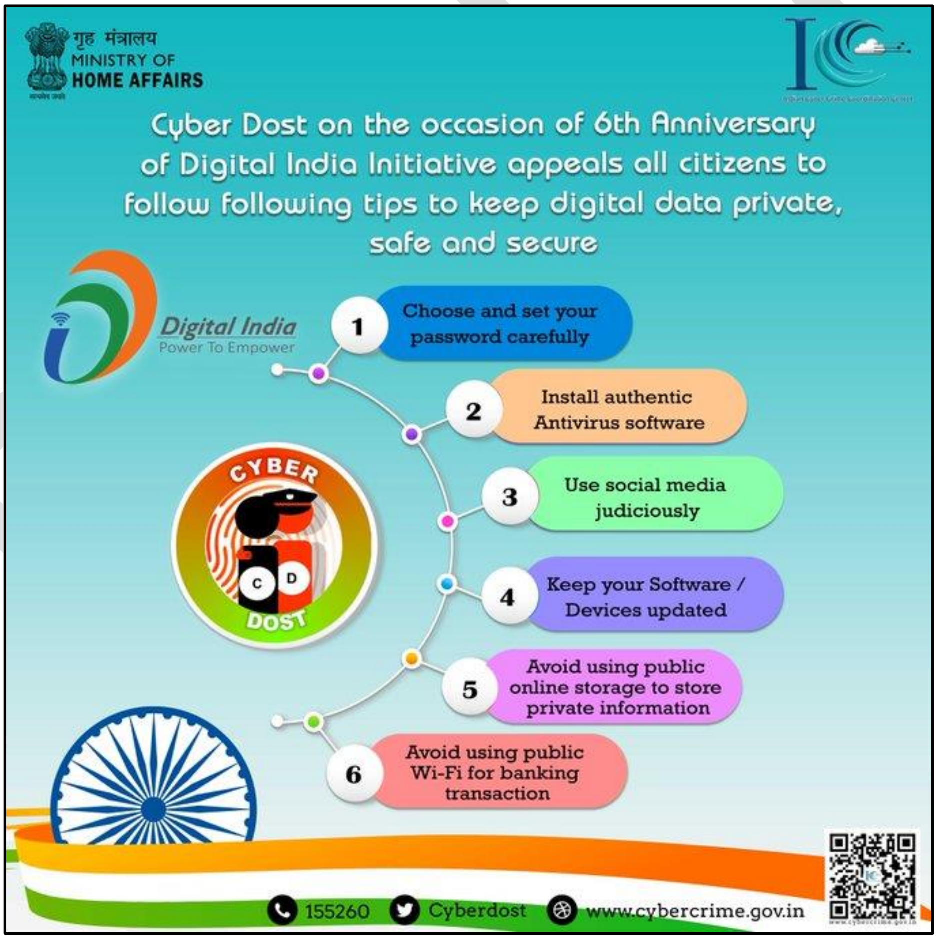
Avoid using same password for multiple devices or accounts

गृह मंत्रालय MINISTRY OF HOME AFFAIRS

फेक न्यूज से सावधान

सोशल मीडिया प्लैटफार्म पर गैर-सत्यापित पोस्टों / खबरों को साझा अथवा अग्रेषित न करें क्योंकि, ये लोगों को गुमराह कर सकती है।

☎ 155260 CyberDost www.cybercrime.gov.in



गृह मंत्रालय MINISTRY OF HOME AFFAIRS

Cyber Dost on the occasion of 6th Anniversary of Digital India Initiative appeals all citizens to follow following tips to keep digital data private, safe and secure

1. Choose and set your password carefully
2. Install authentic Antivirus software
3. Use social media judiciously
4. Keep your Software / Devices updated
5. Avoid using public online storage to store private information
6. Avoid using public Wi-Fi for banking transaction

☎ 155260 Cyberdost www.cybercrime.gov.in

गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS

Indian Cyber Crime Coordination Center

Tips for internet safety

1. Avoid making your personal information public on social media sites and internet in general.

2. Enable privacy safeguards and settings on browsers and major websites such as Facebook, Instagram, Whatsapp etc.

3. Keep your Antivirus Program up-to- date.

4. Always choose strong passwords

गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS

Indian Cyber Crime Coordination Center

Make your Children Aware

a) Cyber bullying is a punishable crime

b) They should never indulge in cyber bullying

c) If anyone teases them, they should inform parents

गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS

Indian Cyber Crime Coordination Center

Watching videos is fun for Kids. But some videos have malicious links that could lead to inappropriate or illegal content. Kids be advised to immediately inform family members, if such activity is noticed.

InfoSec POSTER

NATIONAL CYBER SECURITY AWARENESS MONTH

OCTOBER, 2021

75
Azadi Ka Amrit Mahotsav

Harassment via e-mail

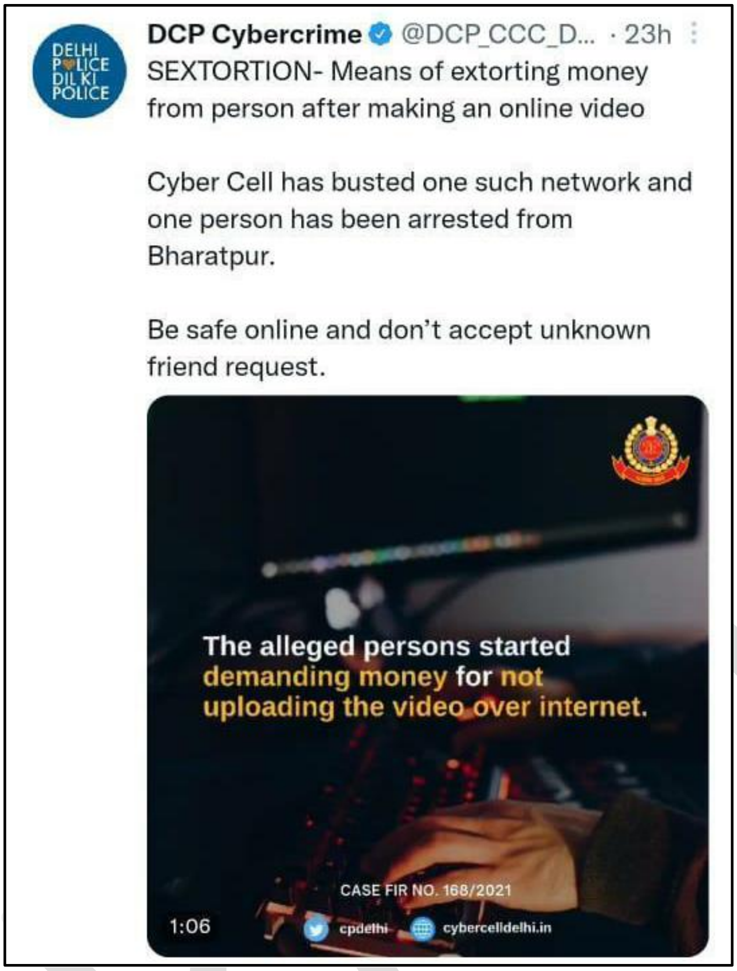
Send the money immediately else I will ruin your life
I know all your secrets !! You have to do whatever I say
You are too ugly Go get a plastic surgery
ha ha ha ..!!! You are done now. You can never get a job

Don't Panic

Save the Evidence &

Report at Cyber Crime Cell

https://infosecawareness.in/c3



DCP Cybercrime @DCP_CCC_D... · 23h

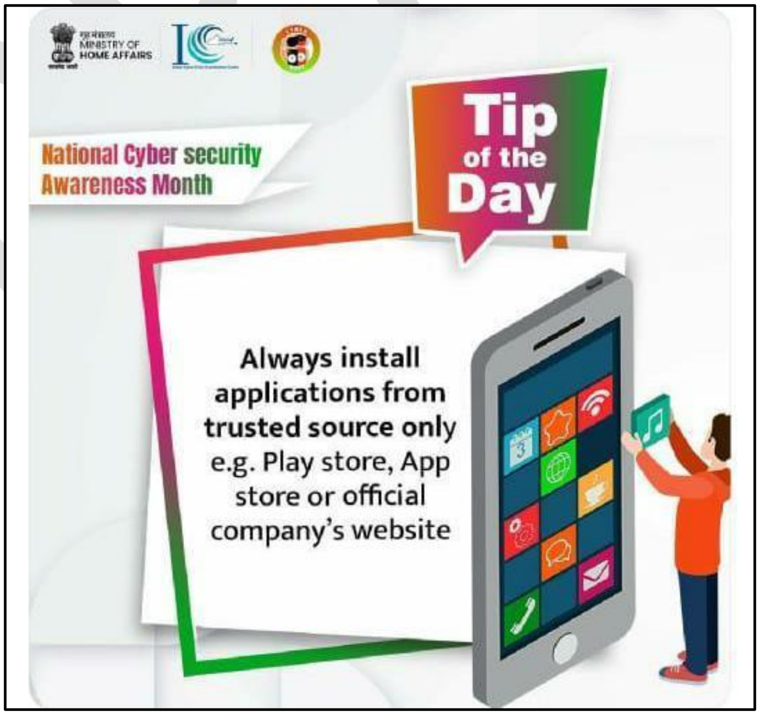
SEXTORTION- Means of extorting money from person after making an online video

Cyber Cell has busted one such network and one person has been arrested from Bharatpur.

Be safe online and don't accept unknown friend request.

The alleged persons started demanding money for not uploading the video over internet.

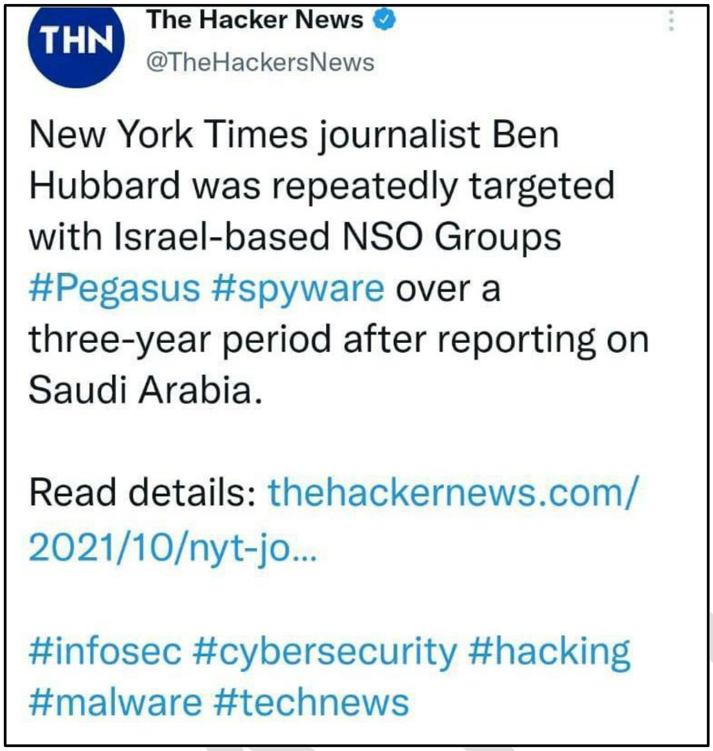
CASE FIR NO. 168/2021



National Cyber security Awareness Month

Tip of the Day

Always install applications from trusted source only e.g. Play store, App store or official company's website

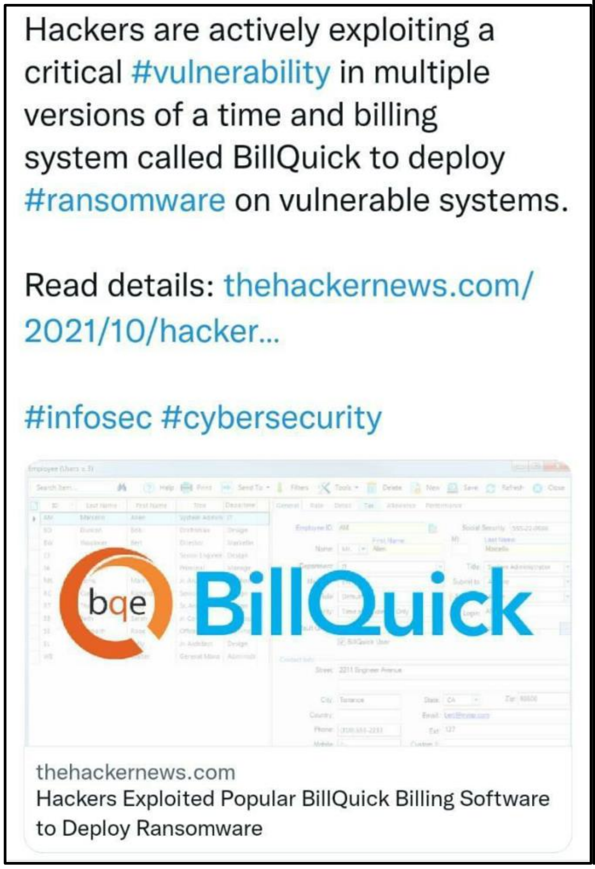


The Hacker News
@TheHackersNews

New York Times journalist Ben Hubbard was repeatedly targeted with Israel-based NSO Groups #Pegasus #spyware over a three-year period after reporting on Saudi Arabia.

Read details: thehackernews.com/2021/10/nyt-jo...

#infosec #cybersecurity #hacking #malware #technews

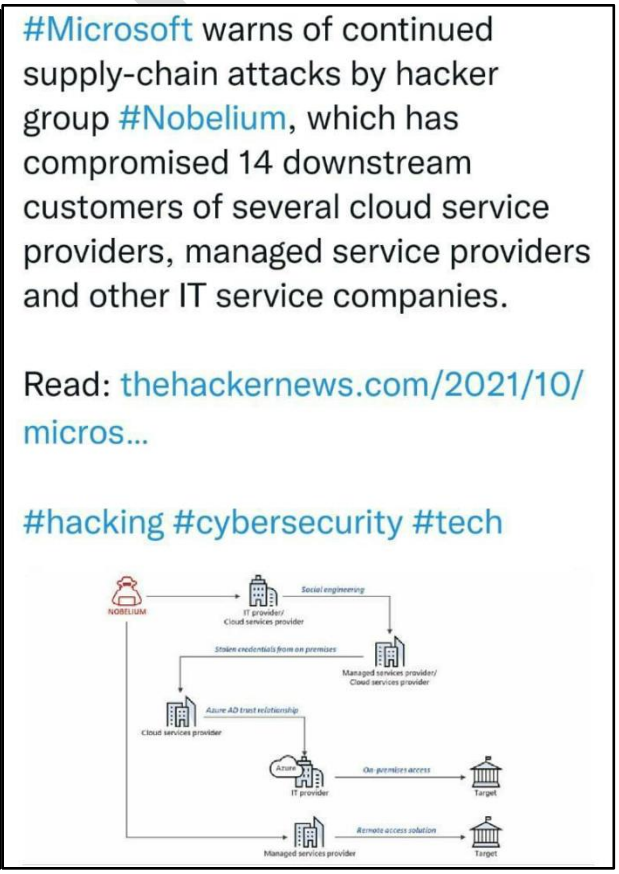


Hackers are actively exploiting a critical #vulnerability in multiple versions of a time and billing system called BillQuick to deploy #ransomware on vulnerable systems.

Read details: thehackernews.com/2021/10/hacker...

#infosec #cybersecurity

thehackernews.com
Hackers Exploited Popular BillQuick Billing Software to Deploy Ransomware



#Microsoft warns of continued supply-chain attacks by hacker group #Nobelium, which has compromised 14 downstream customers of several cloud service providers, managed service providers and other IT service companies.

Read: thehackernews.com/2021/10/micros...

#hacking #cybersecurity #tech

NOBELIUM
IT provider/ Cloud services provider
Social engineering
Stolen credentials from on premises
Managed services provider/ Cloud services provider
Cloud services provider
Azure AD trust relationship
Azure
IT provider
On-premises access
Target
Managed services provider
Remote access solution
Target

REFERENCES

- https://blog.online.colostate.edu/blog/online-teaching/redefining-teaching-the-five-roles-of-the-online-instructor/
- https://www.dqindia.com/big-leap-blackboard-smartboard/
- https://blog.sanako.com/virtual-classroom-security-threats-and-how-to-address-them
- https://csrc.nist.gov/glossary/term/cyberspace
- https://www.nationalarchives.gov.uk/documents/information-management/information-assets-factsheet.pdf
- https://panoply.io/analytics-stack-guide/data-profiling-best-practices/
- https://www.kaspersky.com/resource-center/threats/deep-web
- https://www.tylercybersecurity.com/blog/cyberattacks-101-man-in-the-middle
- https://guides.lib.uw.edu/c.php?g=345925&p=7772376
- https://www.cybercrimechambers.com/
- https://www.geeksforgeeks.org/what-is-information-security/
- http://rmias.cardiff.ac.uk/
- https://tech.hindustantimes.com/tech/news/delhi-police-is-warning-everyone-about-fake-kyc-messages-71621696174975.html
- https://cybercrime.gov.in/pdf/Cyber%20Security%20Awareness%20Booklet%20for%20Citizens.pdf
- https://www.csoonline.com/article/3334617/what-is-spear-phishing-why-targeted-email-attacks-are-so-difficult-to-stop.html
- http://www.cybercelldelhi.in/Fakeshoppingsite.html
- https://gadgets.ndtv.com/how-to/features/online-payment-frauds-upi-apps-e-wallets-how-to-avoid-steps-guide-2384538
- https://www.hdfcbank.com/personal/useful-links/security/beware-of-fraud/sim-swap
- https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/credit-card-fraud
- https://www.financialexpress.com/money/5-strategies-to-safeguard-against-demat-account-frauds/1721683/

- https://constantinecannon.com/practice/whistleblower/whistleblower-types/financial-investment-fraud/cryptocurrency-fraud/
- https://www.open.edu/openlearn/health-sports-psychology/psychology/the-psychology-cybercrime/content-section-2.2.1
- https://www.herts.police.uk/Information-and-services/Advice/Online-safety/Trolling-and-cyberbullying
- https://www.kaspersky.com/blog/online-gamer-threats/4474/
- https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/romance-scams
- http://www.cybercelldelhi.in/mobileapprelatedcrimes.html
- https://www.endnowfoundation.org/detect_matrimony_frauds-php/
- https://cybercrime.gov.in/pdf/Job%20Fraud%20Brochure%20Final.pdf
- https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams
- https://www.itgovernance.co.uk/blog/5-ways-to-detect-a-phishing-email
- https://economictimes.indiatimes.com/tech/internet/making-payments-online-follow-these-10-steps-to-keep-your-money-safe/articleshow/60840679.cms
- https://www.npci.org.in/what-we-do/aeps/product-overview
- https://www.getastra.com/blog/knowledge-base/ecommerce-security/
- https://support.microsoft.com/en-us/windows/keep-your-computer-secure-at-home-c348f24f-a4f0-de5d-9e4a-e0fc156ab221
- https://www.ntiva.com/blog/top-5-mobile-device-security-best-practices
- https://media.defense.gov/2020/Jul/28/2002465830/-1/-1/0/MOBILE_DEVICE_BEST_PRACTICES_FINAL_V3%20-%20COPY.PDF
- https://opensource.com/resources/linux
- https://www.linux.com/what-is-linux/
- https://www.javatpoint.com/advantages-of-linux
- https://www.ncsc.gov.uk/section/about-ncsc/what-is-cyber-security
- https://www.meity.gov.in/content/icert
- http://www.isea.gov.in/
- https://nciipc.gov.in/index.html
- https://www.mha.gov.in/division_of_mha/cyber-and-information-security-cis-division
- http://cwprs.gov.in/WriteReadData/file/cyberdost/cyberdost_twitter_mha.pdf

- https://www.mha.gov.in/division_of_mha/cyber-and-information-security-cis-division/Details-about-CCPWC-CybercrimePrevention-against-Women-and-Children-Scheme
- http://www.cybercelldelhi.in/
- https://www.cdac.in/index.aspx?id=cyber_security
- https://www.drishtiias.com/daily-updates/daily-news-analysis/new-facility-to-tackle-cyber-crimes
- https://www.drishtiias.com/daily-updates/daily-news-analysis/rising-cybercrimes
- https://www.drishtiias.com/daily-updates/daily-news-analysis/national-cyber-security-strategy-2020
- https://www.myadvo.in/blog/how-to-file-a-cyber-crime-complaint-with-cyber-cell-in-india/
  - https://www.researchtrend.net/ijet/pdf/70-S-806.pdf
  - https://startsmarter.co.uk/the-advantages-and-disadvantages-of-digitalisation/
- https://www.fortinet.com/resources/cyberglossary/worm-virus
- https://us.norton.com/internetsecurity-malware-what-is-a-trojan.html
- https://study.com/academy/lesson/what-is-a-backdoor-virus-definition-removal-example.html
- https://www.kaspersky.com/resource-center/definitions/what-is-rootkit
- https://www.pandasecurity.com/en/mediacenter/mobile-news/funeral-directors/
- https://www.mcafee.com/enterprise/en-in/security-awareness/ransomware/malware-vs-viruses.html
- https://www.cisecurity.org/spotlight/cybersecurity-spotlight-spoofing/
- http://www.cybercelldelhi.in/socialmediacrimes.html
- https://www.asurion.com/connect/tech-tips/what-to-do-when-your-phone-is-lost-or-stolen/
- http://www.isea.gov.in/
- https://cytrain.ncrb.gov.in/course/
- https://www.careers360.com/courses-certifications/articles/top-universities-in-india-offering-cyber-security-courses
- https://rems.ed.gov/docs/Cybersecurity_Considerations_for_Higher_ed_Fact_Sheet_508C.pdf

- http://faridkotpolice.in/guidlines.pdf
- https://cybersecurityguide.org/careers/chief-information-security-officer/
- https://ciso.eccouncil.org/cciso-certification/
- https://www.infosectrain.com/courses/cciso-certification-online-training/
- https://www.the420.in/step-by-step-guide-how-to-file-cybercrime-complaint-online-in-india/

Glossary of Terms:

Artificial Intelligence: Artificial Intelligence (AI) is the ability of a computer or a robot controlled by a computer to do tasks that are usually done by humans because they require human intelligence and discernment.

Backup: In information technology, a backup, or data backup is a copy of computer data taken and stored elsewhere so that it may be used to restore the original after an event of data loss.

Bandwidth: In computing, bandwidth is the maximum rate of data transfer across a given path.

Big Data: Big Data refers to extremely large data sets that may be analyzed computationally to reveal patterns, trends, and associations, especially relating to human behavior and interactions.

Biometrics: In information technology, biometrics usually refers to automated technologies for authenticating and verifying human body characteristics such as fingerprints, eye retinas and irises, voice patterns, facial patterns, and hand measurements (NIST, 2015).

Bots: A bot is a computer program that performs automatic, repetitive, and pre-defined activities. Bots are designed to mimic or replace human behavior.

Browsing history: Browsing history refers to the list of web pages where a user has visited, as well as associated with metadata such as page title and time of visit.

CIA Triad: Information security programs are built around three principles, referred to as the CIA Triad - Confidentiality, Integrity, and Availability, where:

- Confidentiality entails not disclosing information to unauthorized individuals, entities, or processes;
- Integrity involves ensuring the accuracy and completeness of data; and
- Availability indicates the availability of information when it is required.

Content Delivery Network: A Content Delivery Network (CDN) is a geographically distributed network of servers and their data centers that help in content distribution to users with minimal delay.

Cryptocurrency: A cryptocurrency is a digital or virtual currency that is secured by cryptography, which makes it nearly impossible to counterfeit or double-spend. For example, bitcoin, litecoin, ethereum, etc.

Cryptography: Cryptography is the discipline that embodies the principles, means, and methods for the transformation of data in order to hide their semantic content, prevent their unauthorized use or prevent their undetected modification (NIST, 2015)

Cyberbullying: Cyberbullying is bullying through digital technology where unpleasant, damaging, and wrong content about someone else can be sent, posted, or shared.

Cyber Espionage: Cyber espionage is an act of intrusion that can give the desired information.

Cyberspace: Cyberspace is a global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers (NIST, 2015).

Cyberstalking: Cyberstalking is a crime when a victim is harassed by the attacker utilizing e-mail, Instant Messaging (IM), internet messages, discussion groups, etc., to communicate electronically with the victim.

Cyberwar: Cyberwar refers to the actions by a nation-state to penetrate another nation’s computers or networks for the purpose of causing damage or disruption (Clarke and Knake, 2010).

Data accessibility: Data access refers to a user's ability to access or retrieve data stored within a database or other repository.

Data Breach: A data breach occurs when malicious insiders or external attackers gain unauthorized access to confidential data or sensitive information such as medical records, financial information, or personally identifiable information.

Data profiling: Data profiling is the process of reviewing source data, understanding structure, content, interrelationships, and identifying potential for data projects.

Data Diddling: Data diddling is a type of cybercrime in which data is altered as it is entered into a computer system, most often by a data entry clerk or a computer virus.

Decryption: The conversion of encrypted data into its original form is called Decryption.

Deep Fakes: Deep Fakes is a new and complex type of audio, video, or image disinformation that is typically used for malicious purposes. They can quickly spread fraudulent words and actions to a global audience, and they can be difficult to tell apart from genuine information.

Demat Account: Demat Account is short for dematerialization account and makes the process of holding investments like shares, bonds, government securities, mutual funds, and insurance easier, eliminating the hassles of physical handling and maintenance of paper shares and related documents.

Denial of Service (DOS): Denial of service (DoS) is a type of cyber-attack designed to disable, shut down or disrupt a network, website, or service. Typically, malware is used to interrupt or inhibit the normal flow of data into and out of a system to render the target useless or inaccessible for a certain period.

De-parameterisation: De-parameterisation is protecting an organization's systems and data on multiple levels by using a mixture of encryption, secure computer protocols, secure computer systems, and data-level authentication, rather than the reliance of an organization on its network boundary to the Internet.

Digital currency: Digital currency is a form of currency that is available only in digital or electronic form. It is also called digital money, electronic money, or electronic currency.

Digitalization: Digitalization is the use of emerging technologies such as Artificial Intelligence, Machine Learning, the Internet of Things, etc. to modify a business model and generate new revenue and value-producing opportunities.

Distributed Denial-of-Service (DDoS): It is a cybercrime in which the attacker floods a server with internet traffic to prevent users from accessing connected online services and sites

Distributed network: A distributed network is a type of computer network that is spread over different networks. This provides a single data communication network, which can be managed jointly or separately by each network

Domain name: A domain name is an easy-to-remember name that's associated with a physical IP address on the Internet. For instance, the domain name google.com might translate to the physical address *198.102.434.8*.

E-commerce: The term electronic commerce (e-commerce) refers to a business model that allows companies and individuals to buy and sell goods and services over the Internet.

Encryption: Encryption is the process of encoding a document or data so that only individuals with access to a secret key, password, or token can open and decrypt (make readable) the information.

Extranet: An extranet is a controlled private network that allows access to partners, vendors, and suppliers or an authorized set of customers, normally to a subset of the information accessible from an organization's intranet.

Financial Fraud: Financial fraud occurs when someone steals one’s money or else harms one’s financial health by deceitful, dishonest, or unlawful tactics. This can be accomplished through a variety of means, including identity theft and investment fraud.

Firewall: A firewall is an inter-network gateway that restricts data communication traffic to and from one of the connected networks and thus protects that network's system resources against threats from the other network (NIST, 2015).

Hacker: Unauthorized user who attempts to or gains access to an information system.

Hacking: Hacking is the activity of using a computer to access information stored on another computer system without permission, or to spread a computer virus (Cambridge Dictionary).

Hoax email: An email hoax is a scam that is distributed in email form. It is designed to deceive and defraud email recipients, often for monetary gain. Hoaxes are emails typically arriving in chain letter fashion that often describe impossible events, highly damaging malware.

Identity/Credential Theft: Identity theft is the obtaining of some other person's personal information without their permission. Personal information may contain a person's name, phone number, address, bank account number, Aadhaar number, credit/debit card number, passwords among other things.

Impersonation: Impersonation is used as a technique where basic credentials are stolen. The threat actor or bad actor pretends to be someone else by adopting that person's identity to get access to resources, credit, or other benefits in that person's name and fame.

Information Assets: An information asset is a collection of data that is defined and managed as a single unit, allowing it to be easily understood, shared, safeguarded, and exploited. A contact database is an excellent example of a single information asset.

Information security: Information security is the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. Cyber security is a specific type of information security that refers to the ways in which organizations protect digital information, such as networks, programs, devices, servers, and other digital assets.

Inspection: Inspection refers to the examination of an information system to determine compliance with security policy, procedures, and practices (NIST, 2015).

Intranet: An intranet is a computer network for sharing information, easier communication, collaboration tools, operational systems, and other computing services within an organization, usually to the exclusion of access by outsiders.

Intrusion: Intrusion involves stealing valuable resources and jeopardizing the security of systems, networks, devices, or data, as the case may be.

Keylogger: Keyloggers are activity-monitoring software programs that give hackers access to the user's personal data such as passwords, credit card numbers, or the web pages they visit, by logging the keyboard strokes.

Law Enforcement Agency (LEA): A law enforcement agency (LEA) is any government agency responsible for the enforcement of the laws.

Logic Bombs: A logic bomb is a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met.

Machine Learning: Machine learning is a subset of artificial intelligence that provides systems the ability to automatically learn and improve from experience without being explicitly programmed.

Man-In-The-Middle: Man-in-the-Middle (MITM) attacks occur when an attacker intercepts communications between two parties. These attacks allow attackers to intrude and eavesdrop on the communication or data transfer between the two targets, as well as change the traffic flowing between them.

Margin funds: Margin funds refer to a short-term loan facility that investors use to make up for any shortcomings that they encounter, while trading or when purchasing stocks, at a predetermined rate of interest.

Misinformation/Disinformation: Misinformation is simply false information that is disseminated, whether or not the purpose is to deceive, whereas disinformation is intentionally misleading or biased information that is based on distorted narratives or facts to achieve propaganda.

Morphing: Morphing is the process of smoothly transitioning from one image to another without any changes using online morphing tools.

Multi-Factor Authentication (MFA): An authentication system that requires more than one distinct authentication factor for successful authentication (NIST, 2015).

National Nodal Agency: National Nodal Agency has been set up for all measures to protect the nation's critical information infrastructure.

Nodes: A node is a basic unit of a data structure, such as a linked list or tree data structure. Nodes contain data and also may link to other nodes.

Outsourcing: Outsourcing is a business practice in which a company hires a third party to perform tasks, handle operations or provide services for the company.

Phishing: A phishing attack is a means of tricking people into disclosing confidential information by answering an email. It involves obtaining or attempting to gain specific banking information (e.g. username, password, credit card numbers, etc).

Remote access control: Remote access control refers to the ability to monitor and control access to a computer or network (such as a home computer or office network computer) anywhere and anytime.

Rootkits: A rootkit is a kind of software that allows hackers to gain access to and command over a computer.

Server: A server is a computer or device on a network that manages network resources. Examples include file servers (to store files), print servers (to manage one or more printers), network servers (to manage network traffic), and database servers (to process database queries).

Skimming: Skimming is an illegal practice used by identity thieves to capture credit card information from a cardholder surreptitiously. Fraudsters often use a device called a skimmer that can be installed at gas pumps or ATM machines to collect card data.

Social Engineering: Social engineering assaults usually include psychological manipulation to persuade unaware users. It involves sending an email or other message to a target that elicits feelings of urgency, fear, or other comparable emotions, prompting the victim to reveal sensitive information, click a harmful link, or open a malicious file.

Spoofing: Spoofing occurs when cyber threat actors try to hide their true identities by faking the sender of a message to regularly fool the recipient into thinking it came from someone else.

Spyware: Spyware is defined as malicious software designed to enter a computer device, gather data about the person, and forward it to a third party without consent.

SSL Certificates: An SSL certificate is a digital certificate that authenticates a website's identity and enables an encrypted connection. SSL stands for Secure Sockets Layer, a security protocol that creates an encrypted link between a web server and a web browser.

Supply-chain attack: A supply chain attack is an attack that allows the adversary to utilize implants or other vulnerabilities inserted prior to installation in order to infiltrate data, or manipulate information technology hardware, software, operating systems, peripherals (information technology products), or services at any point during the life cycle (NIST, 2015).

Trojan: A Trojan horse, often known as a Trojan, is malicious malware or software that appears to be legal yet can take control of the computer.

Worm: A worm virus is a harmful program that duplicates itself and spreads through a network automatically. The worm virus exploits flaws in the security software to steal important information, install backdoors that can be exploited to access the system, corrupt files, and perform other types of harm.

Abbreviations Used:

ABBREVIATIONS USED	FULL FORMS
ACH	Automated Clearing House
AePS	Aadhaar Enabled Payment System
ATM	Automated Teller Machine
CD	Compact Disc
CDSL	Central Depository Services Limited
CISO	Chief Information Security Officer
CVV	Card Verification Value
EFT	Electronic Funds Transfer
GPS	Global Positioning System
GST	Goods and Services Tax
HEI	Higher Education Institution
HTTPS	Hypertext Transfer Protocol Secure
IT	Information Technology
KYC	Know Your Customer
MMS	Multimedia Messaging Service

NATGRID	National Intelligence Grid
NISPG	National Information Security Policy and Guidelines
NSDL	National Securities Depositories Limited
OLX	On-Line eXchange
OTP	One-Time Password
PCs	Personal Computers
PDF	Portable Document Format
PIN	Personal Identification Number
PoS	Point of Sale
SIM Card	Subscriber Identity Module Card
SMS	Short Message Service
UPI	Unified Payments Interface
URL	Uniform Resource Locator
USB	Universal Serial Bus