Information Security Education & Awareness
Ministry of Electronics and Information Technology
Government of India

InfoSec Newsletter

NOVEMBER 2021

Cyber Offences that are Sexual in Nature -Vol II

For Virus Alerts,Incident & Vulnerability Reporting
certin Handling Computer Security Incidents
www.cyberswachhtakendra.gov.in

सी डैक CDAC प्रगत संगणन विकास केन्द्र
CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING
इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय की वैज्ञानिक संस्था, भारत सरकार
A Scientific Society of the Ministry of Electronics and Information Technology, Government of India
Plot No: 6&7, Hardware Park Sy. No.1/1, Srisailam Highway Raviryal (V & GP), Via Ragaanna guda, Maheshwaram (M), Ranga Reddy District, Hyderabad – 501510. Tel: 9248920201.

InfoSec Newsletter

NOVEMBER 2021

CREDITS

Honorary Professor. N Balakrishnan
(IISc, Bangalore)
Prof. Sukumar Nandi
(IIT, Guwahati)
Prof. V Kamakoti (IIT, Madras)
Prof. M S Gaur (SVNIT, Jaipur)

Design & Technical Team
Ch A S Murty
K Indra Veni
K Indra Keerthi
Kinjal Pitroda

Action Group Members
HoD (HRD), MeitY
Shri.Sitaram Chamarthy (TCS)
Prof. M S Gaur (MNIT, Jaipur)
Prof. Dr.Dhiren R Patel
(NIT Surat)
Representative of Chairman
(CBSE)
CEO, DSCI (NASSCOM)
Representative of Prasar Bharati,
Member of I & B
Shri U Rama Mohan Rao
(SP, Cyber Crimes, CID,
Hyderabad, Andhra Pradesh)
Shri S K Vyas, MeitY

Compiled by
Ch A S Murty
M Jagadish Babu
Simi P

From C-DAC
Mrs P R Lakshmi Eswari, Director

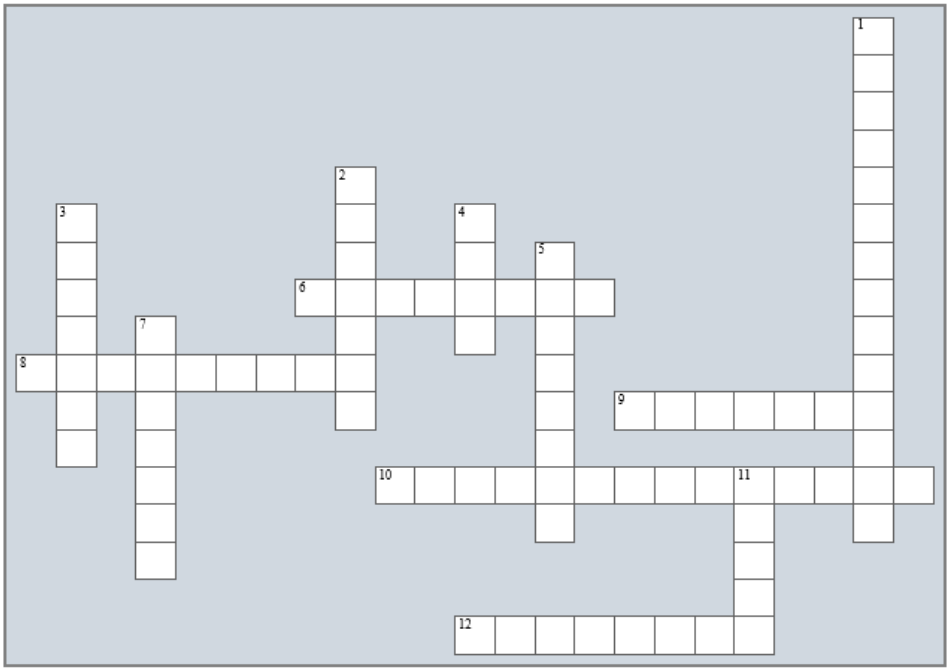
Acknowledgement
HRD Division
Ministry of Electronics &
Information Technology

Supported by

For Virus Alerts,Incident & Vulnerability Reporting
certin
Handling Computer Security Incidents

InfoSec ACTIVITY

InfoSec CROSSWORD



DOWN

1. Intimidating online behavior, where the user is targeted on public platform with threatening, humiliating, embarrassing and harassing posts.
2. Children should immediately inform their _____ or trusted adults, if something or someone makes them feel uncomfortable online.
3. You should not befriend _____ people online without properly verifying their details.
4. Technology today can prove to be a wonderful and exciting _____, provided you know how to use it safely.
5. A string of characters/ secret phrase used to gain access to a digital device.
7. A type of malware that can send information about your data to an attacker.
11. You should never open mails or click on _____ received from unverified/ unknown sources.

ACROSS

6. _____ Information should never be shared publicly online.
8. If you receive offensive material or threatening mails/messages online, seek from friends and family, and register _____ on portal www.cybercrime.in or with local law enforcement agency/ cybercrime cell.
9. Users should enable their _____ and Security features on social media platforms to ensure safety.
10. Constant monitoring of your online activities and tracking your where abouts online.
12. Never share your personal/private _____ online with everyone publicly, as they can be used for morphing.

InfoSec JUMBLED WORDS

1. USE **UDAETPD RSOTAFWE** - _____
2. USE **SROTNG SSAPRODWS** - _____
3. USE **ALIREWLF** AND **TIANVIUSR** - _____
4. ENABLE **STAFYE AND SUCERITY FAEUTRSE** - _____
5. DO NOT **SRHAE PRESNOLA IFONRAMTOIN** - _____
6. DO NOT **BEFIREDN SRTANEGSR** YOU MEET **LIONNE** - _____

InfoSec TIC - TAC - TOE

Strike a line through the three similar cyber offences terms given in the grid either vertically, horizontally or diagonally.

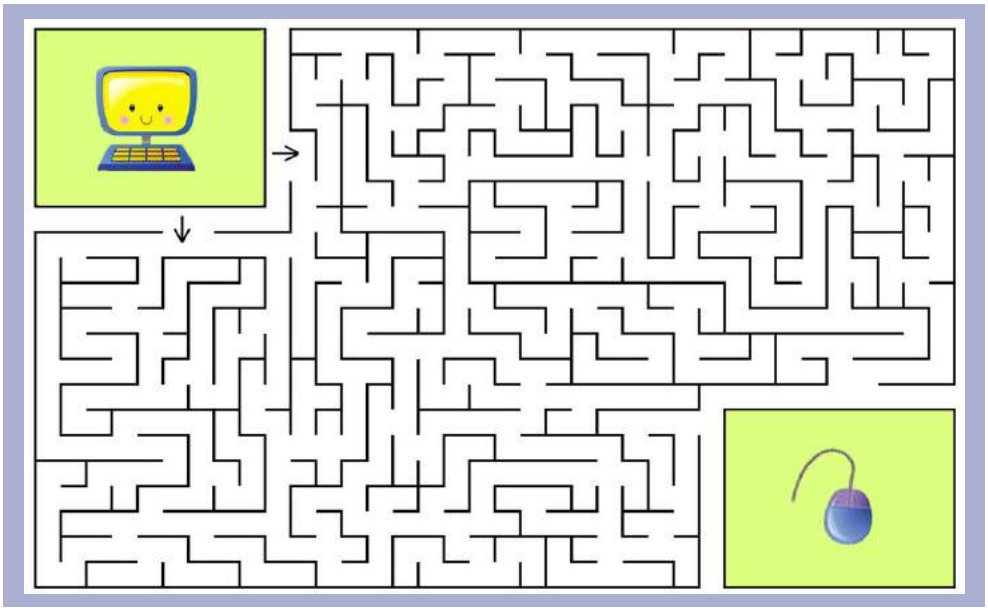
Morphing	Malware	Hardware
Trojan	Stalking	Keyboard
Monitor	Software	Bullying

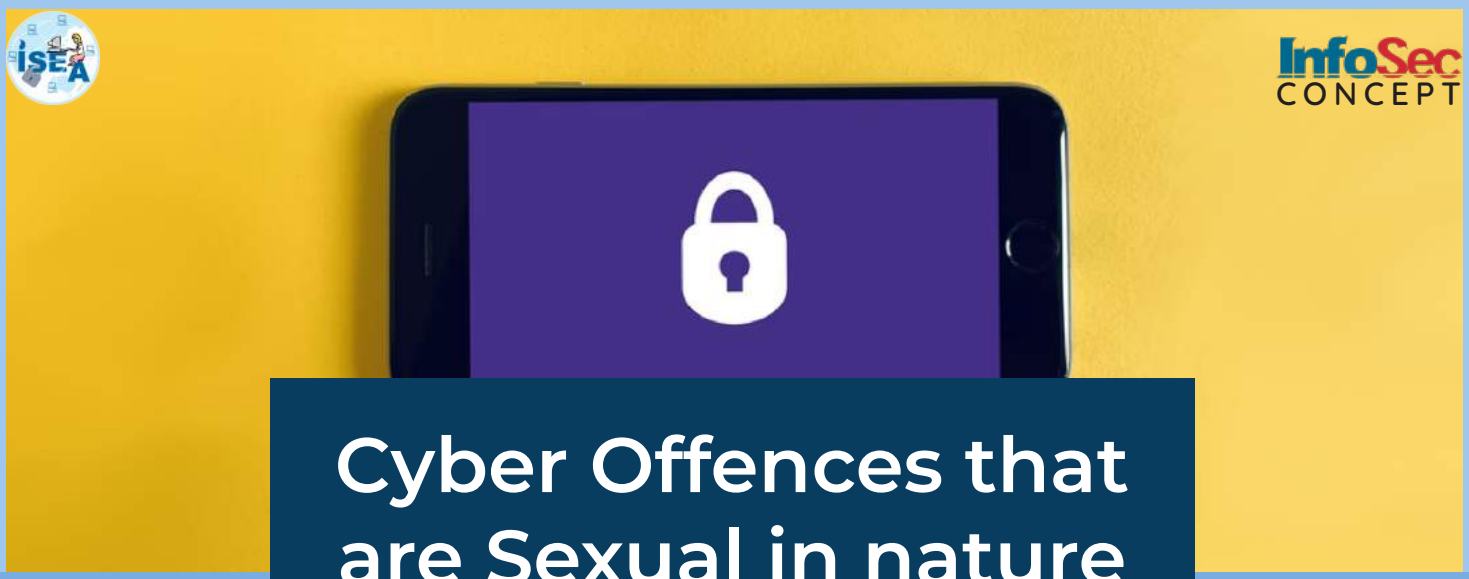
Webcam Protection	Antivirus	Security Features
Strong Password	Multifactor Authentication	Two factor Authentication
Printer	Updated Software	Finger print Scanner

InfoSec FIND THE DIFFERENCES

Find five differences.

InfoSec FIND THE WAY





Cyber Offences that are Sexual in nature

How do they effect the vulnerable groups and what are the online safety tips for protection ???

Cyber Age the technology driven economies & individuals

Scope and Risks of digital devices usage

Today in the 'cyber age' that we live in, the usage of digital devices with internet has become a norm. The efficiency, affordability and pervasiveness of technology have made it an integral part of our daily lives. The power of internet based technology has been able to charge and give boost to every sphere of economy revolutionizing business, banking, commerce, communication, education, entertainment and other services. This scenario has pushed every individual to adopt the digital lifestyle at a very quick pace that was never seen before.

In the current digital times, the access to technology through convenience of digital devices is far reaching and has touched every aspect of our daily life. Today internet enables its digital users to create content and communicate with each other across the globe in matter of seconds. The digital users today use pictures, video, sound, and text to share their real lives, genuine identity etc. The Internet has allowed individuals to free themselves from the geographic limitations and come together in topic-based communities that are not tied down to any specific place - Personal stories can go public and local issues can become global now.

While this rapid growth of information highway on one hand has opened doors for gaining vast knowledge, explore new horizons and access new ways to communicate, interact and use services, it has also led to new forms of online crimes or cyber offences threatening the privacy and security of the netizens. Wide range of cyber offences have been noticed to be taking place in the cyber space, which can broadly be divided into two categories i.e., cybercrimes that target networks or devices with the virus/-malware/DDOS attacks and the cybercrimes that use digital devices to commit criminal activities, which include phishing attacks, cyber stalking, Identity theft etc.,. These attacks lead to financial loss, data breach, system/network hacking, online account hacking, online harassment etc., causing grave distress, personal and financial loss to the digital consumers.

Women and Children – soft targets for cyber criminals

Cybercrimes disproportionately affect the vulnerable sections, especially women and children. Cybercrimes like stalking, online harassment and bullying, sexting, etc., have suddenly acquired wide currency after the cyber space has become more populated and instruments to perpetrate these crimes in the cyber space have become widespread. These crimes are difficult to trace and investigate because they are anonymous. As per the statistical data published by National Crime Records Bureau (NCRB), last during 2019, the cybercrimes in India have registe-red a 63.5% jump over 2018, this shows the alarming rate at which the cybercrimes are increasing in the country. It is also noted that cyber crimes related to sexual exploitation raised by 5.1% during the period. According to the report submitted in Rajya Sabha by the Parliamentary Standing Committee on Home Affairs on 'Atrocities and Crimes Against Women and Children', the cybercrimes against women and children have doubled in 2019. As per the report there were 8684 cases crimes registered in 2019, as against 4330 cases in 2017. Also the report mentions that, the major cyber crimes noted against women and children as reported by NCRB are cyber blackmailing/threatening, cyber pornography / hosting, cyber stalking / bullying, defamation/-

morphing, fake profile, etc.,

The penetration and wide spread use of the technology powered by internet, lack of awareness on safe & hygienic digital practices, anonymity of perpetrator in cyber space, misuse of technology, tools & resources by fraudsters in different ways to commit offences, easy access to data or individual information etc., can be termed as few of the reasons for the growth of cybercrimes. It is essential that thedigital users especially women and children are made aware of hygienic digital practices to be followed to ensure security in the Digital space. Also, they need to be made aware about different types of the cybercrimes that may affect them, the related dangers, their warning signs, modus operandi and safety measures to protect themselves against such crimes. In addition to these, every cyber citizen should also be knowledgeable about the ways to approach law in case of victimization and the provisions available under the law to seek help and justice.

Information on few of the critical cybercrimes generally seen against women and children like Fake profiles, Cyber stalking, Sextortion, Morphing, Cyber bullying, Child pornography are briefly being shared here with appropriate examples to make the readers and stakeholders aware on such grave and serious instances of cybercrimes against women and children.

Let us look into each of these Online Sexual Offences and understand its implications and ways to handle it.

Few Cyber Crimes against Women and Children:

Fake profiles
Cyber stalking
Sextortion
Morphing
Cyber bullying
Child pornography

FAKE PROFILE

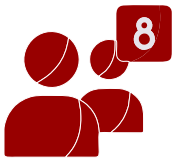
When cyber fraudsters create a social media profile using the identity details like name, address, mail id, photograph etc., of victim, without their knowledge, it is called a fake profile creation.

The fraudsters create fake profile with an intention of causing harm to the victim. The fraudsters use the fake profile to spread false or fake information, damage the reputation of the victim, and may also send friend requests to other friends of victim to gain financial benefit.

Dangers of Fake profile

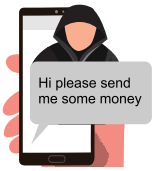
Spreads false and fake information

Damage reputation

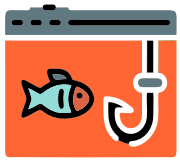


Sends false friend requests.

Lure children and teenagers with fake identity



Financial fraud may also happen by requesting money using messenger

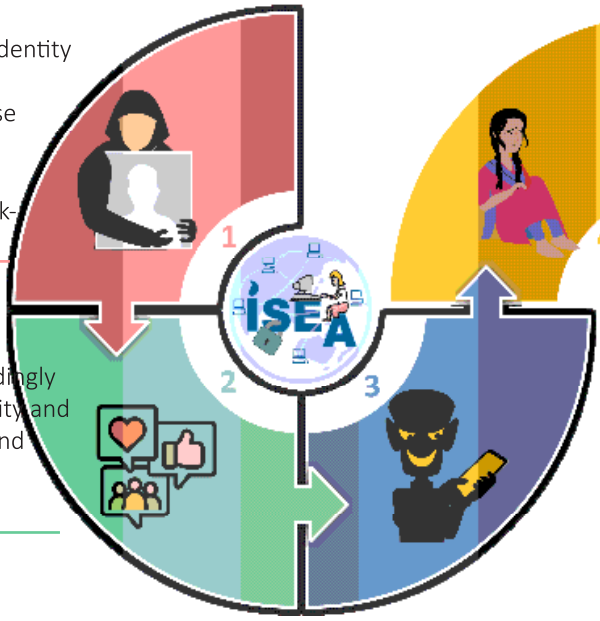


Makes the friends and family of victim vulnerable to cyber-attacks like phishing

Modus Operandi

1 Fraudsters chooses a fake identity as per his requirement
Either a fictional one or false identity of others
Ex. army personnel; popular personalities; professional working abroad etc.,

2 They create a profile accordingly with the chosen false identity and contact the victim/s and send friend requests.



With the fake social media profile created they can

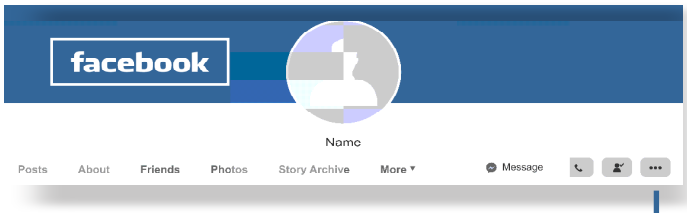
- send friend requests to the victim to trap them
- post false messages to damage the reputation of the person being impersonated
- request for money/gifts; show false romantic interests for money ; try to sell false goods/items etc.,
- The culprits does everything to earn their trust of the victims through the fake account and then trap them.

The victim suffers in various ways through the fake social media account it can be

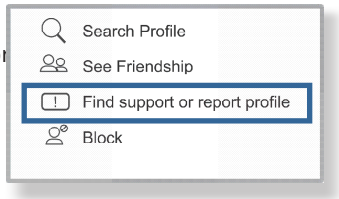
- monetary loss
- loss of reputation and public image
- trapped into fake relationships etc.,

How to report regarding the fake profiles

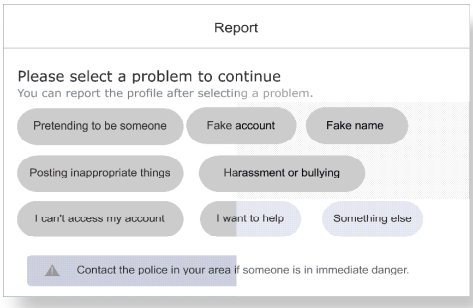
If its Facebook



Step 1
Go to the specific fake account in Facebook and click on three dots on the right side



Step 2
Click on Find support or



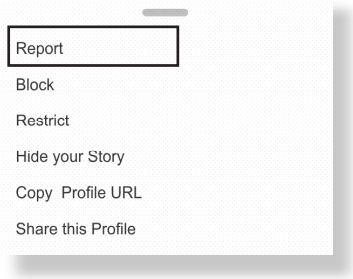
Step 3
Choose the appropriate options from

visit the URL https://www.facebook.com/report/ to know more about how to report .

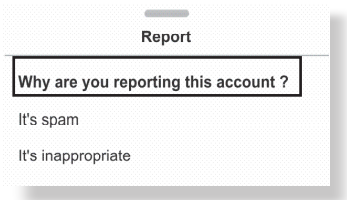
If its Instagram Account

Step 1
Go to the fake account that is opened in Instagram

Step 2
Click on the three dots on the top right hand side corner of profile page



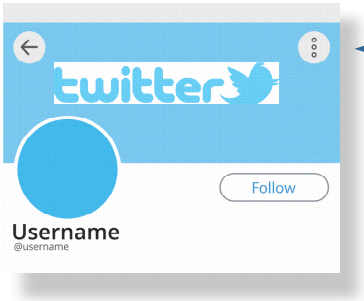
Step 3
Select the option Report



Step 4
for the question 'why are you reporting this account', select the options 'its inappropriate account'

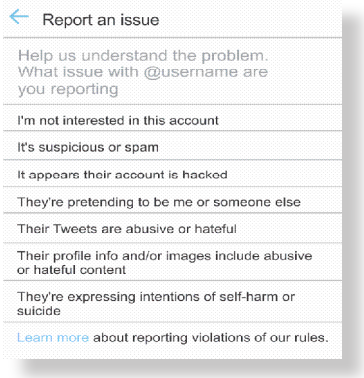
visit the URL https://help.instagram.com/ to know more about how to report

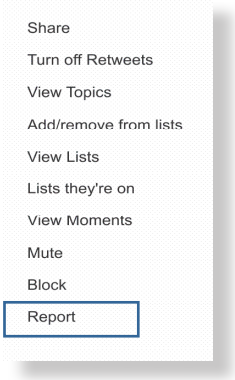
If its Twitter Account



Step 1
Go to the specific fake account in Twitter and click on three dots on the right side

Step 2 Select the option 'they are pretending to be me or someone





Step 3
Select the appropriate option from "Report an

visit the URL https://help.twitter.com/en to know more about how to report .

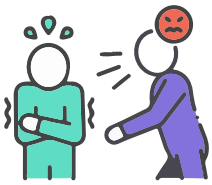
CYBER STALKING

A cyber stalker makes use of internet and electronic means to monitor your online activities and track your whereabouts to harass, intimidate, embarrass, accuse, threaten, commit identity theft or malware attack.

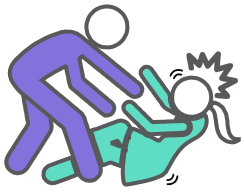
The cyber stalker starts harassing you anonymously using online means like your email, social networks, instant messaging etc.,. They can intrude on your privacy and can track your physical location and cause harm. They can take control of your online accounts and can spread false rumors about you online.

Dangers of Cyber Stalking


Intrusion of privacy


Intimidation


Online harassment

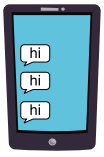

Danger of physical attack / harm


Anxiety, fear and distress

Warning signs of Cyber Stalking

Frequent and multiple messages over a period of time

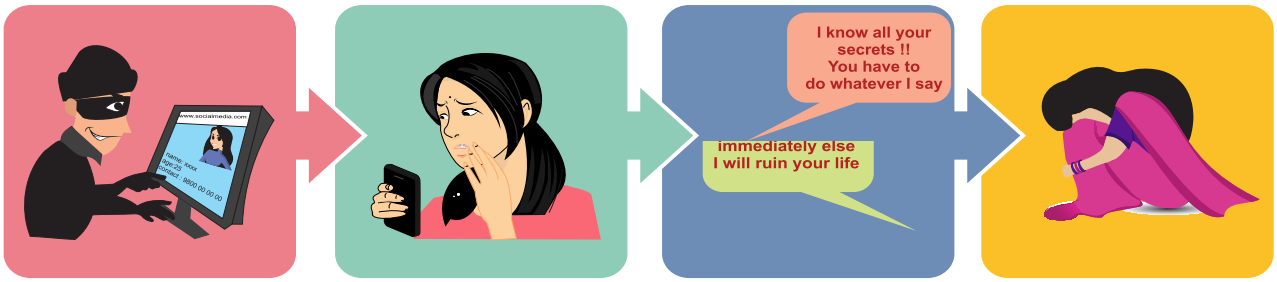

Posts with inappropriate content and has details of your whereabouts or personal aspects.



Sending repeated emails


Constantly follow you over your social media accounts.

Modus Operandi



The victim is constantly monitored online through their social media accounts and some times physically too, by the stalker.

The victim may receive unsolicited mails/posts/ comments/messages/ calls from the stalker.

The stalker may try to create threat in the mind of the victim.

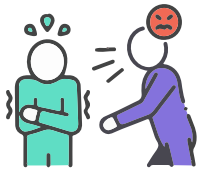
The victim is constantly harassed with obscene posts/ images/threats etc., by the stalker.

ONLINE SEXTORTION

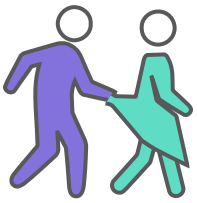
Online Sextortion occurs when a fraudster threatens to circulate your private and sensitive material online, if you do not provide images of a sexual nature, sexual favors, or money. The perpetrator may also threaten to harm your friends or relatives by using information they have obtained from electronic devices unless you comply with their demands.

Sextortion is a form of online abuse, wherein the cybercriminal makes use of various channels like instant messaging apps, SMS, online dating apps, social media platforms, porn sites etc., to lure the users into intimate video/audio chats and makes them pose nude or obtains revealing pictures from them. The fraudsters later make use of this material to harass, embarrass, threaten, exploit and blackmail the victims.

Dangers of Online Sextrotion

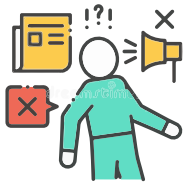


Abuse & Exploitation



Harassment

Blackmail



Threats of public humiliation

Mental distress

Modus Operandi

01 The fraudsters try to lure the users into sharing intimate content in different ways:

-Posting messages for video/audio chat
-Using fake accounts/profiles
-Creating pages/ad campaigns

02 The users get victimized when they:

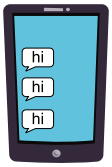
-Pay for such services and pose nude or in compromising position in video call.
-Accepts or sends friend requests to the fake account/profile and involves in intimate interaction posing nude in video chats, sends revealing pictures etc.

03 The fraudster records video/ takes screen-shot/ takes pictures/makes use of revealing pitures/ morphs the pictures sent.

04 The fraudster starts blackmailing the victim leading to sextortion.

The users of porn sites may also fall prey sextortion, when their chats/ video calls on the porn sites are used for blackmailing by fraudsters.

Channels used for trapping the victims



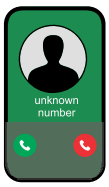
Instant Messaging apps

Dating apps

Social media platforms

Porn sites, etc.,

Warning signs indicate attempts of sextortion



Repeated untoward messages/video calls from unknown number/s

Repeated friend requests from unknown person

Repeated request for private intimate pictures, video chats, photos

Manipulating or redirecting the conversation towards intimate topics

Rush through the things and trying to develop intimacy

Warning signs that may indicate victimization

Signs of fear, nervousness, anxiety, depression

Isolating self and being very reactive & emotional

Feeling desperate and frustrated

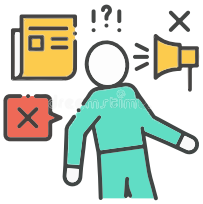
Having suicidal thoughts and self-harming behavior.

MORPHING

Morphing is altering or changing the pictures of the person using morphing tools available online. Young girls and women usually fall prey at the hands of the online criminals, who use their photographs posted online and misuse these images by changing the pictures.

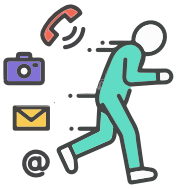
The altered pictures are then used by perpetrators for blackmailing you, creating fake online profile, sexting, sex chats, pornographic content, nude pictures etc.,

Dangers of Morphing

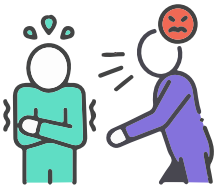


Damage to reputation

Emotional trauma



Blackmailing



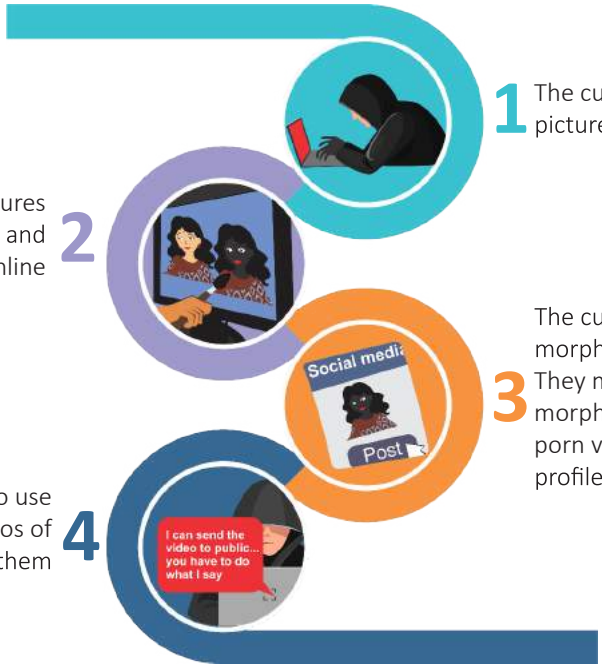
Public humiliation

Degrading remarks & messages online

Warning signs of Morphing

Messages/comments/remarks/calls from people and from unknown numbers.

Modus Operandi



1 The culprit gains possession of the pictures of the victim

2 The culprit changes the pictures of victim using online tools and circulates it online

3 The culprit attempts to misuse the morphed pictures of the victim. They make use of the morphed pictures in porn sites, porn videos, movies, fake online profiles, sexting etc.,

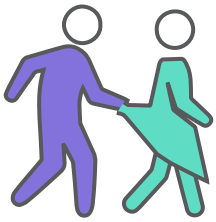
4 The culprit may also use these morphed pictures/videos of victims to blackmail them

CYBER BULLYING

Cyber bullying is intimidating online behavior, wherein you can be targeted on an online public platform with threatening, humiliating, embarrassing and harassing posts or acts.

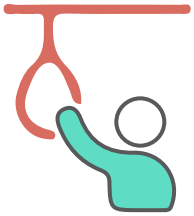
Dangers of Cyber Bulling

Social isolation



Harassment

Mental stress



Suicidal thoughts

Warning signs of Cyber Bulling

Recurrent health issues and not eating well

Avoiding school or college and isolating self

Feeling depressed, sad, worried, agitated

Loosing interest in doing any activities

Modus Operandi

1

The adult/child becomes a victim

2

He/she is targeted by his/her class mates or other members online in the group.

3

Perpetrator uses extreme harsh words targeting the vicitm.

4

The adult/ child and the victim may be mercilessly trolled and targeted with humiliating, intimidating, derogatory online posts.

CHILD PORNOGRAPHY

Online Child pornography is the abuse or exploitation of a minor (below 18 years) in a sexually explicit act/conduct online through images or videos. The online predators lurking in social media platforms, gaming sites, chat rooms, lure and trick children and adolescents into situations with the motive of sexual abuse/exploitation.

Dangers of Child Pornography

Depression

Distress

Self isolation

Feelings of guilt, shame and wrong doing

Extreme physical pain

Emotional disturbance

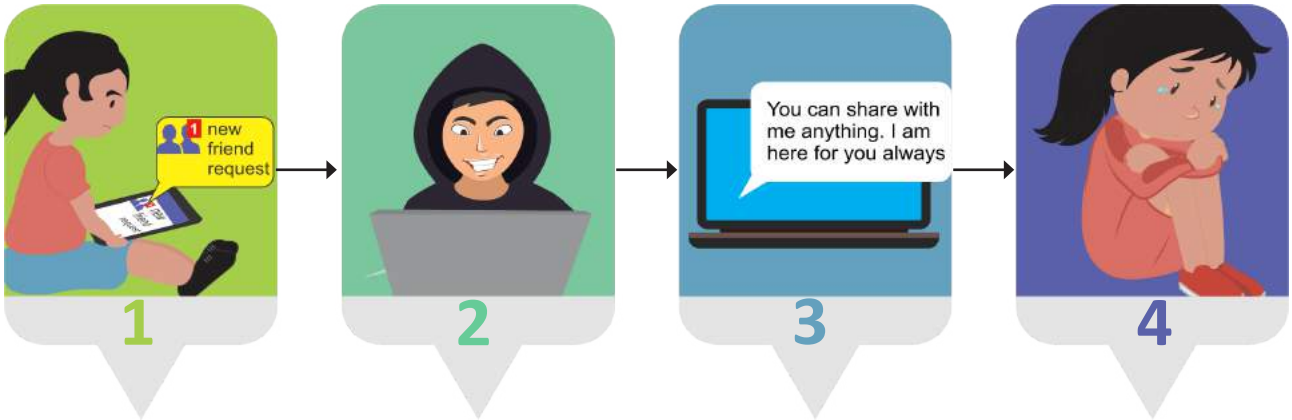
Warning signs of Child Pornography

The child can be burdened by feelings of guilt and wrong doing, shame etc.,

The child undergoes extreme physical pain and emotional disturbance

The child remains sad, distressed, isolated and may show signs depression.

Modus Operandi



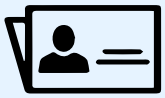
1. The online predators contact children on online platforms like chatrooms/ gaming sites/social media platforms.
2. They try to connect to children with fake identity and win their trust
3. They build an emotional connect and convince children with their exceptionally friendly behaviour, with motive of sexual abuse and exploitation
4. They convince or coerce children into performing sexually explicit acts.

Good online practices to safeguard against such kind of cyber offences

In the current scenario it becomes extremely necessary for both the parents and children to be aware and alert about such crimes and accordingly know the measures to safeguard against such crimes.

Safety tips while sharing personal information

1. Avoid sharing your personal information like address, mobile number, personal mail id and other sensitive identity related information on social media and restrict access.



2. Share groups pictures rather than Individual images and post limited information only in the social media platforms

3. Do not share your personal high resolution pictures online publicly on social media accounts

4. Never share any compromising images, posts, videos of yourself to anyone, no matter who they are

Safety tips while interacting with others online

Never send money to the requests sent on social media accounts, also call to verify before paying.

Never accept friend requests from unknown persons without appropriate verification and confirmation.

Never click on suspicious links or download anything until you verify the authenticity of the source.

Be alert of any queries about your online actions that you are not aware about.

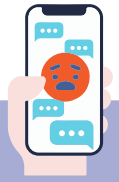
Always be alert what your online friends are commenting on your photos or any activities, block the strangers/unknown people sending undue comments.

During an online interaction or chat, if the person on the other side is trying to rush through the things and develop intimacy, then it is cause of alarm.

Never allow anyone, however close to capture any private part or intimate activity with any device. Such a data can be misused at a later stage.

Do not accept video calls or open attachments from people you do not know.

Leave the discussion page and block the bully, when you find negative/provocative posts.



Never retaliate to the provocative comments of the bully, understand that others reaction is not your fault.

Reach out for help, talk to your parents and friends immediately.

If an online contact is being too good to you, claiming to share same interests, likes & dislikes and shows interest in meeting you personally, it is a warning sign.

Never agree to personally meet a stranger who has befriended you online, without informing the parents.

Educate children on secured digital practices and dangers of befriending online strangers.

In case you experience something uncomfortable, immediately cutoff all contacts with this person, inform your parents and report on cybercrime.gov.in.

Safety tips for improved security of your online accounts

Be aware of security and privacy features and enable them on the social media accounts. It is better to restrict privacy setting to family and known friends only. https://www.facebook.com/help/; https://help.twitter.com/en; https://help.instagram.com/; https://faq.whatsapp.com/ (Select the privacy and security options in the given URL's links and follow instructions)

Always disable your GPS from your device if you are not using it. Also disable location on social media account.

Turn off your electronic devices and web cameras when you are not using them.

If you observe your fake profile or any such objectionable post on social media, report on the social media help center about it. To know more visit Social Media Help Centre URLs: https://www.facebook.com/help/; https://help.twitter.com/en; https://help.instagram.com/

Avoid clicking intimate/nude/semi-nude photos/videos on your phone, which if leaked could cause embarrassment. There are several rouge mobile apps that could access your gallery/storage and can be used to blackmail you.

Use different passwords for different social media accounts and emails.

Use "Report User" option over social media platforms to report any fake accounts.

Enable Two Factor (2FA) or Multi Factor Authentication (MFA provided by the social media platforms.

How to report against such offences

Do not suffer in silence, know that you are not alone, reach out and seek help from trusted family and friends.

Save the evidence and the screen shots for referring to the incident later.

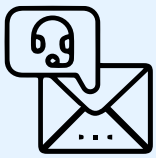
File a complaint against sextortion or such online offences at your nearest cybercrime cell personally or file an online complaint on portal www.cybercrime.gov.in

Remember that you can also anonymously file an online complaint against such offence on the national cybercrime reporting portal www.cybercrime.gov.in.

Don't hesitate in filing a complaint or contacting police due to shame, embarrassment and self-blame, this will only encourage the perpetrator to carry on with their crime.

You can contact the social media administrators (Facebook, twitter etc.,) and report to them regarding any inappropriate post.

Contact the helpline number 1098, provided by Ministry of Women and Child Development.



Register a complaint at your nearest cybercrime police station.
Refer to site www.cybercrime.gov.in for contact details of Cybercrime Police Stations across India*

InfoSec LATEST NEWS

Google releases Chrome upgrade Chrome 93: multi-Screen window placement, PWAs as URL handlers, and more the newest Chrome beta channel release for Android, Android Web View, Chrome OS, Linux, macOs, and Windows
visit at https://blog.chromium.org/

Google bans 8 dangerous apps from Play Store; DELETE them from your phone now
https://tech.hindustantimes.com/tech/news/google-bans-8-dangerous-apps-from-play-store-delete-them-from-your-phone-now- check-list-71629565818495.html

InfoSec VIRUS ALERTS

CERT-In Vulnerability Note CIVN-2021-0281
Denial-of-Service Vulnerability in Siemens RUGGEDCOM ROX Devices

Software Affected
RUGGEDCOM ROX MX5000, RX1400, RX1500, RX1501, RX1510, RX1511, RX1512, RX1524, RX1536, RX5000 versions prior to 2.14.1

Overview
A Vulnerability has been reported in Siemens RUGGEDCOM ROX Devices which could be exploited by an attacker to cause denial of service condition on the targeted system.

Description
This vulnerability exists in Siemens RUGGEDCOM ROX devices due to writing crash dumps without checking if enough space is available on the file system.

Successful exploitation of this vulnerability could allow the attacker to cause Denial-of-Service attack on the targeted system.

For more details visit: https://cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES01&VLCODE=CIVN-2021-0281

CERT-In Advisory CIAD-2021-0040
Remote code execution vulnerability in Apache HTTP Server

Systems Affected
Apache HTTP Server version 2.4.49 and 2.4.50

Overview
A vulnerability has been reported in Apache HTTP Server which could be exploited by a remote attacker to execute arbitrary code on the targeted system.

Description
This vulnerability exists in Apache HTTP server due to an insufficient fix for the path traversal vulnerability (CVE-2021-41733).A remote attacker could exploit this vulnerability by sending specially crafted request to map URLs to files outside the directories configured by Alias-like directives.

Successful exploitation of this vulnerability could allow the attacker to execute arbitrary code, if CGI scripts are also enabled for these aliased paths, and may result in complete compromise of vulnerable system.

For more details visit: https://cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES02&VLCODE=CIAD-2021-0040

CERT-In Vulnerability Note CIVN-2021-0282
Multiple vulnerabilities in Advantech WebAccess

Systems Affected
Advantech WebAccess versions 9.02 and prior

Overview
Multiple vulnerabilities have been reported in Advantech Web Access which could be exploited by a remote attacker to execute arbitrary code on the targeted system.

Description
These vulnerabilities exist in Advantech WebAccess due to improper bound checking. A remote attacker could exploit these vulnerabilities by sending a specially-crafted request.

Successful exploitation of these vulnerabilities could allow a remote attacker to trigger buffer overflow and execute arbitrary code on the targeted system.

For more details visit: https://cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES01&VLCODE=CIVN-2021-0282

CERT-In Advisory CIAD-2021-0039
Multiple Vulnerabilities in Apache HTTP Server

Systems Affected
Apache HTTP Server version 2.4.49

Overview
Multiple vulnerabilities have been reported in Apache HTTP Server which could be exploited by a remote attacker to execute arbitrary code or cause denial of service conditions on the target system.

Description
1. Directory traversal Vulnerability (CVE-2021-41773).
The vulnerability exists in Apache HTTP Server due to incomplete path normalization logic implemented. A remote attacker could exploit this vulnerability by sending specially crafted requests to map URLs to files outside the expected document root. Successful exploitation of this vulnerability could allow a remote attacker to traverse directories on the system, if files outside of the document root are not protected by "require all denied" these requests can succeed. This vulnerability could also expose the source of interpreted files like CGI scripts, which may be used for further attacks.

Note: This issue is currently exploited in the wild, users are advised to upgrade urgently.

2. Denial of Service Vulnerability (CVE-2021-41524).
This vulnerability exists in Apache HTTP Server due to NULL pointer dereference error in HTTP/2 requests. A remote attacker could exploit this vulnerability by sending a specially crafted request to perform a denial of service (DoS) condition on the targeted system.

For more details visit: https://cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES02&VLCODE=CIAD-2021-0039

For queries on Information Security
Call us to Toll Free No.

1800 425 6235

For details on
Cyber Crime Cells in India and Cyber Crime Reporting Portal
visit https://www.infosecawareness.in

To Share Tips / Latest News, mail us to

isea@cdac.in

About ISEA

Looking at the growing importance for the Information Security, Ministry of Electronics & Information Technology has identified this as a critical area. Information Security Education and Awareness (ISEA) Project was formulated and launched by the Govt. of India. One of the activities under this programme is to spread Information Security Awareness among children, teachers, home users, IT and non-IT professionals throughout the country. C-DAC Hyderabad has been assigned the responsibility of executing this project by Ministry of Electronics & Information Technology, Government of India. As part of this activity C-DAC, Hyderabad has been preparing Information Security Awareness material, coordinating with Participating Institutes (PI's) in organizing the various Information Security Awareness events all over India.

About C-DAC

C-DAC established its Hyderabad Centre in the year 1999 to work in Research, Development and Training activities embracing the latest Hardware & Software Technologies. The centre is a Knowledge Centre with the components of Knowledge Creation, Knowledge Dissemination and Knowledge Application to grow in the areas of Research & Development, Training and Business respectively. The R & D areas of the centre are e-Security, Embedded Systems, Ubiquitous Computing, e-Learning and ICT for Rural Development. The centre has developed over a period of time a number of products and solutions and has established a number of labs in cutting edge technologies. In line with these R&D strengths, the centre also offers Post Graduate level diploma courses. Centre is also actively involved in organizing faculty training programs. The centre regularly conducts skill based training and information security awareness programmes. InDG portal is hosted and maintained to facilitate rural development through provision of relevant information, products and services in local languages.

BOOK POST

For queries on Information security

Call us on Toll Free No.

1800 425 6235

between 10.00 AM to 6.00 PM
or give us a missed call
we will call you back within 24 hrs

ISEA Whatsapp Number for Incident Reporting

+91 9490771800

Between 9.00 AM to 5.30 PM

Subscribe us on

https://www.youtube.com/c/InformationSecurityEducationandAwareness

Follow us on

https://twitter.com/InfoSecAwa

Connect us with

https://www.facebook.com/infosecawareness

Ministry of Electronics & Information Technology,
Government of India

सी डैक CDAC प्रगत संगणन विकास केन्द्र
CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING
इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय की वैज्ञानिक संस्था, भारत सरकार
A Scientific Society of the Ministry of Electronics and Information Technology, Government of India
Plot No: 6&7, Hardware Park Sy. No.1/1, Srisailam Highway Raviryal (V & GP), Via Ragaanna guda, Maheshwaram (M), Ranga Reddy District, Hyderabad – 501510. Tel: 9248920201.