सत्यमेव जयते

A Handbook for Adolescents/ Students on Cyber Safety

Ministry of Home Affairs
Government of India

A Handbook for Adolescents/ Students on Cyber Safety

Ministry of Home Affairs
Government of India

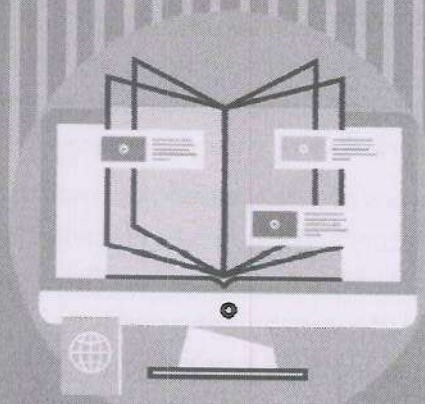
This booklet has been prepared in consultation with Cyber Security experts.

Published by:
Ministry of Home Affairs,
Government of India,
North Block,
New Delhi - 110001

Disclaimer

The information provided in this Handbook is intended to create awareness among citizens especially students about various cyber threats that can impact them and ways to safeguard themselves against cyber crimes. The information, techniques and suggestions given in the Handbook are for general guidance only. In case you become a victim of cyber crime, contact your local police station or state cyber crime cell.

CONTENTS



ABOUT THE HANDBOOK

Information and communication technology has become an integral part of our day-to-day life. It has just transformed the way we communicate, make friends, share updates, play games, and do shopping and so on. The technology has impacted most aspects of our day-to-day life.

Our new generation is getting exposure to cyber space at a very young age. More and more children invest time online to play games, make friends, and use social networking sites and so on. In fact with smart phones access to social networking, online games, shopping, etc. has increased significantly. The cyber space connects us virtually with crores of online users from across the globe. With increasing use of cyber space, cyber crimes are also increasing rapidly.

Children are highly vulnerable as they are exposed to cyber space with limited understanding of cyber threats and safeguards. Children are in experimental age group. They like to experiment, learn new things and use new technologies. While experimenting is a good way to learn, it is equally important that proper guidance is provided to children so that they can protect themselves from adverse impact of cyber technology.

This handbook is for children above 13 years of age. It can be used by younger students as well to understand the cyber world

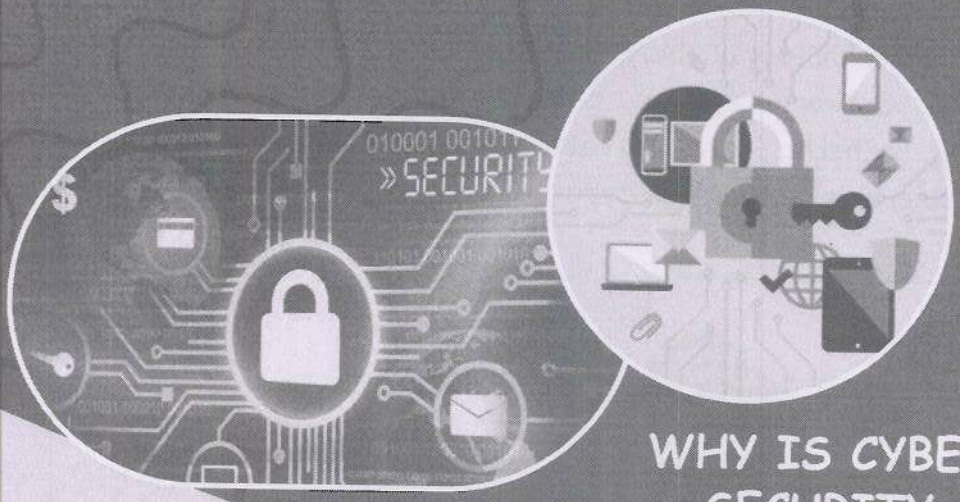
better and prepare themselves to be responsible and careful cyber citizens of future. The purpose of this handbook is to provide an overview of various cyber threats that can impact children and discuss safeguards that can help in preventing the cybercrimes.

The first and second chapters of the handbook provides an insight to children on why cyber security is a concern and what are different types of cybercrimes that can impact us.The third chapter of the handbook talks about cyberbullying and how it can impact children. It further details out the key safeguards that may help children to protect themselves against cyberbullying and ways to deal with cyberbullying.

The fourth chapter of the handbook covers cyber grooming and its impact on the children. It also provides details about various safeguards that can be adopted by children to protect themselves from cyber grooming. The fifth chapter talks about cyber threats related to online gaming and safety tips that can help children in safeguarding themselves against such cyber threats. Emails are used commonly by cybercriminals. The sixth chapter provides an overview of how cybercriminals can trigger cybercrimes using emails and safety tips that may help children in using emails securely.

Cyber technology has also transformed the way we do financial transactions. More and more people are using online platforms for shopping, transferring money and other financial transactions. Moreover, efforts are being made to facilitate financial education in schools in order to make students ready for future. In view of increasing cybercrimes related to financial frauds, chapter seventh of the handbook provides an overview to children on cyber threats related to online financial transactions and how to safeguard ourselves against such threats. The last chapter of the handbook covers cyber threats related to social networking and how to safeguards against such threats.

The handbook shall help students to learn about cyber threats and ways how they can protect themselves. As a change agent, students are expected to share their learning with their peers and parents and contribute in making cyber space safer.



WHY IS CYBER SECURITY A CONCERN?

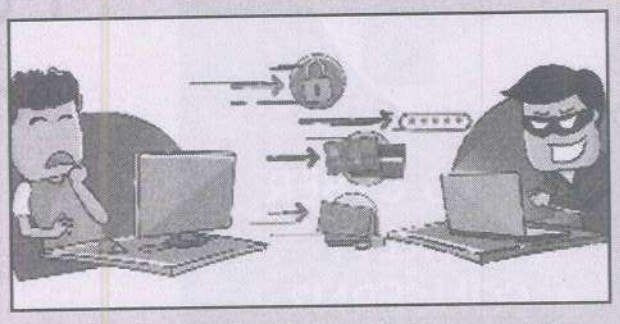
Today internet, computers, smart phones and other communication technology devices have become an integral part of our life. Imagine, how much time we spend each day on these smart devices. We have made internet communication mediums like Google, emails, WhatsApp, Twitter, Facebook, etc., part and parcel of our everyday activities. But most of us are unaware of cyber safety and security essentials to safeguard ourselves.

Do you know that whatever information or personal details are shared on internet stay online forever as it is extremely difficult to delete the information completely?

WHAT ARE CYBER CRIMES?

Cybercrimes are offences that may be committed against individuals, companies or institutions by using

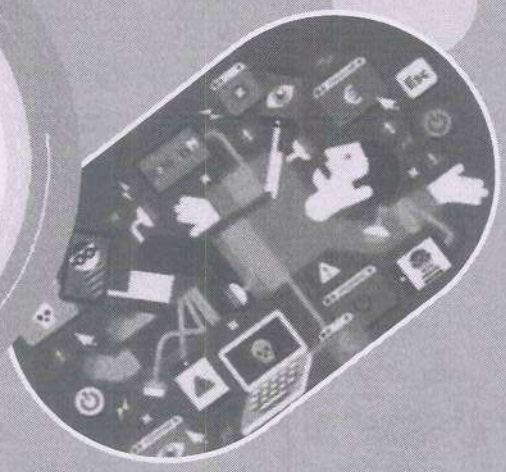
computers, internet or mobile technology. Cybercriminals use platforms such as social networking sites, emails, chatrooms, pirated software, websites, etc., to attack victims. Children are also vulnerable to various types of cybercrimes.



"According to the Indian Computer Emergency Response Team (CERT-In), over 53000 cases of cyber security incidents were reported in 2017 in India"

Do you know that cyber-attacks are becoming more complex and sophisticated and are increasingly targeted on stealing the personal information such as phone number, address, photographs, bank details etc.? The personal information can be used by cyber criminals against you in different ways like creating you fake profile, cyber bullying, etc.

Don't worry friends, by following precautions and being vigilant, you can safeguard yourself against cyber crimes. I am your Cyber Dost and I will help you in understanding various types of cyber crimes and precautions that you must take in order to reduce the risk of falling a victim to cyber crime.



CYBER THREATS THAT CAN IMPACT ANYONE

Cyber threats are different possible ways that can be used to attack us using internet or mobile technology.

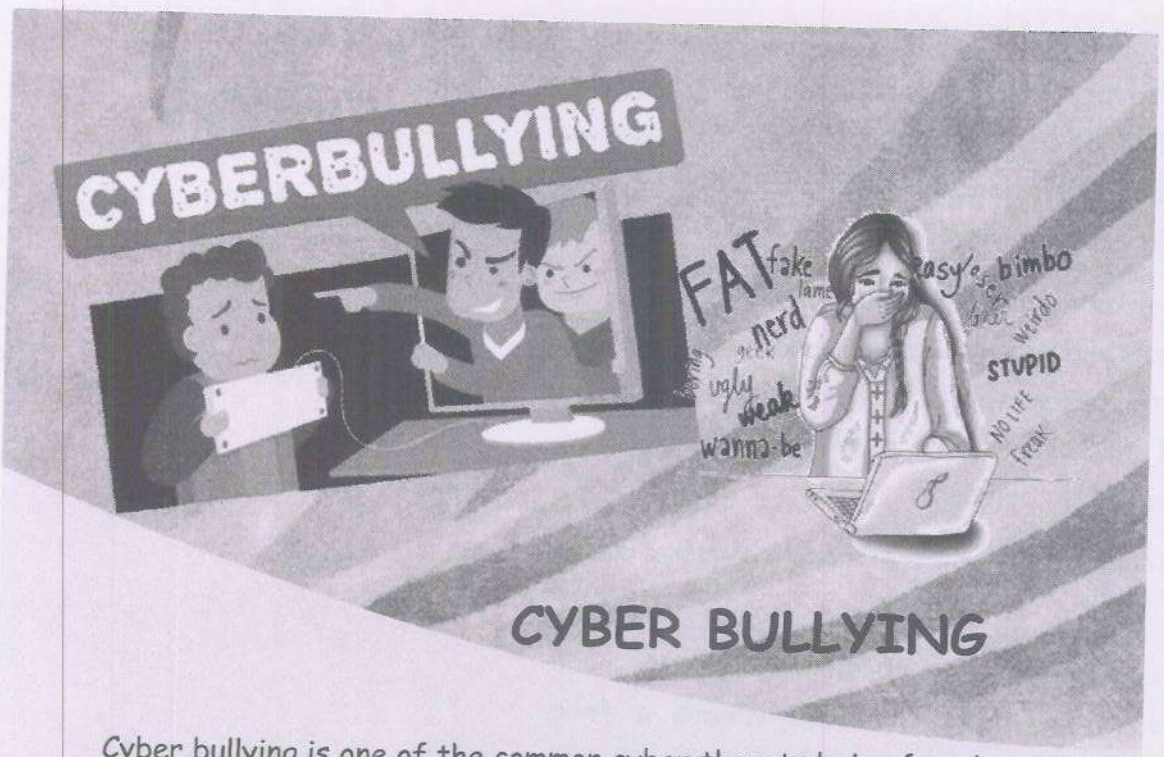
Do you know a hacker is anyone who uses/ exploits technology for an unintended use thereby disrupting operations or causing financial/ reputational lossto people? Hackers can use malwares, viruses or Trojans to attack your computer and gain access to your data.

Cyber criminals want to get unauthorized access to our sensitive information .In majority of cases, the cyber criminals would advent an attack with a clear cut objective, for that they use some of the most effective methods.

Some common ways used by cyber criminals are:

☞ **Email Spoofing:** Sending out e-mails to you that look like genuine and from a trusted e-mail ID but actually, they're not.

- **Malicious Files Applications:** Sending you malicious and bad applications and files through direct messaging, gaming, emails or websites etc. in order to get access to your smart phone and personal data.
- **Social Engineering:** Social Engineering is a technique used by cybercriminals to gain your confidence to get information from you. Depending on what you like to do most, a cybercriminal may try to interact with you to mine for information and/or commit some harm to you. Suppose you like to play an online game, an impersonator behaves like another child and invites you to talk to him and share information.
- **Cyber Bullying:** A form of harassment or bullying inflicted through the use of electronic or communication devices such as computer, mobile phone, laptop, etc.
- **Identity Theft:** Deliberate use of someone's identity to gain financial advantage or to obtain credit and other benefits in the other person's name/ for counterparts disadvantage or loss.
- **Job Frauds:** Fraudulent representation or a deceptive activity on the part of an employee or a prospective employee toward an employer.
- **Banking Frauds:** Fraudulently obtaining money from depositors by posing as a bank or other financial institution.



CYBER BULLYING

Cyber bullying is one of the common cyber threats being faced by children and young people. Though cyber bullying can impact anyone yet due to limited understanding about cyber threats, children become easy victims of cyber bullying.

Cyber bullying means using internet or mobile technology to intentionally harass or bully someone by sending rude, mean or hurtful messages, comments and images/videos. A cyber bully can use text messages, emails, social media platforms, web pages, chat rooms, etc. to bully others.

Do you know that initially we don't even realize that someone is bullying us online? A cyber bully can be a known person, friend, relative or even an unknown person whom we met online on social media platform or a chat room, gaming portal, etc. The magnitude of cyber bullying can range from sending rude and hurtful messages, spreading embarrassing rumours to direct threats, stalking, etc.

The consequences of cyber bullying on children are manifold. There can be physical, emotional and psychological consequences that can not only impact the academic performance of students but affect their daily life to a great extent.

Concerned about cyber bullying? Don't worry... with awareness and precautions you can use internet and mobile technology without any fear. You need to be careful and follow safeguards to protect yourself and your friends against cyber bullying.

Let's discuss how you can protect yourself from becoming a victim of cyber bullying

- Don't accept friend requests from unknown people on social media platforms. Cyber bully can even create a fake account to befriend victims. As a rule of the thumb, only add people online whom you know offline
- Don't share your personal information like date of birth, address, and phone number on social media or other online platforms. You can go to privacy settings on social media platforms to select who can access your posts online. Try to restrict access of your profile to your friends only. Picture stories for example on a particular platform are public by default.
- Remember what you post online remains there so it is important to be careful and not to share your phone number and other personal details in comments or posts on social media platforms
- Never install unwanted Software and Apps like dating App, online games, etc. from unknown sources. You should be very careful while chatting in the chat rooms. Never share

personal details in the chat room and limit your identity.

- If you feel hurt after reading a post from a friend or a stranger, don't react with aggressive reply. It may encourage the bully to keep posting such messages. If hurtful post/message is from your friend, you can request him not to do it again. If you are repeatedly getting such messages/ post, please inform your parents or elders immediately so that they can support you.

- Also, please remember that as a good netizen you should never share mean comments or hurtful messages or embarrassing pictures/videos online. Please be careful and check if your post/comment /videos can be embarrassing for your friend or anyone else. If so, please don't post. You should not become a cyber bully yourself as it is a punishable offence. It adversely impacts the victim.

What can you do if you are a victim of cyber bullying?

If you feel that you are a victim of cyber bullying, please inform your elders so that they can intervene and support you. Following suggestions can be helpful in managing the situation.

- **Inform your parents/elders immediately:** If someone is bullying you, you must inform your parents/elders immediately. Don't feel that your parents will restrict your online activity or ask you not to use your computer/smartphone. It is important to inform them so that they can support and guide you. Narrate the entire issue clearly to your parents/elders.

- **Identify the bully:** Try to identify if the bully is a known person or a stranger. You should try to find out the reason why bully is bothering you. A bully can be your friend or a known person. You may seek help of your parents/teachers to reach out to the bully and ask him/her to stop bullying you.

- **Block the Bully:** If bully is using social media platforms to bully you, you can block him/her. All the social media apps or services have the option to block a user.

- **Collect and Save posts/messages:** Save posts/messages that were used against you. Such messages/posts can be used as an evidence, if in case a legal action has to be taken.

- **Never respond to a bully aggressively:** Bully wants you to get aggressive and get into heated argument. This adds mileage to the information unwantedly. So the best way is to ask the person politely to stop it and if he/she becomes annoying, stop the chat/ block him/ her

- If your parents/elders feel the need, they can contact local police station to lodge a complaint against the bully

Do you know that it is both illegal and unethical to threaten someone online? Even if you send them offensive messages, call them vulgar names, make comments on how they look, etc., you may be calling for trouble.

Cyber Grooming

Cyber Grooming is growing as one of the major cyber threats faced by children and teenagers. It is a practice where someone builds an emotional bond with children through social media or messaging platforms with an objective of gaining their trust for sexually abusing or exploiting them.

The cyber groomers can use gaming websites, social media, email, chat rooms, instant messaging, etc. by creating a fake account and pretending to be a child or having same interests as of the child.

Do you know that many of us don't even realize that someone is grooming us online? Online groomer can be a known person, a relative or even an unknown person whom we met online on social media platform, a chat room or gaming portal, etc.

Initially, the cyber groomer can give you compliments, gifts, modelling job offer and later they can start sending obscene messages, photographs or videos and will ask you to share your sexually explicit images or videos with them.

The online groomer mostly target teenagers as in adolescence they face immense biological, personal and social changes. The

impulsive and curious nature of adolescents encourages them to engage in online activities which makes them vulnerable to online grooming.

The cyber grooming has deep impact on a child's physical, emotional as well as psychological well-being. It can not only impact their academic performance but also their daily life to a great extent. The devastating effects of online grooming can sometimes be long-term and can even haunt the victim in their adulthood

Concerned about cyber grooming? Don't worry... with awareness and precautions you can use internet and mobile technology without any fear. You need to be careful and follow safeguards to protect yourself and your friends against cyber grooming.

Let's discuss how you can protect yourself from becoming a victim of cyber grooming

- Don't accept friend request from unknown people on social media platforms. Cyber groomer can even create a fake account to befriend victims.
- Don't share your personal information like date of birth, address, phone number and school name on social media or other online platforms. You can go to privacy settings on social media platforms to select who can access your posts online. Try to restrict access of your profile to your friends only.
- Be cautious when your chat partner gives you many compliments regarding your appearance in just a short span of your acquaintance.
- Avoid talking to people who asks you questions related to your physical or sexual experiences. You can tell the person to stop asking you such questions as you feel uncomfortable. If they continue to do the same, immediately inform your parents.

- Do not talk to people who ask you to share your sexually explicit photographs or videos. If you share your sexually explicit photos or videos with someone, the person can share those photos with others or post them on social media. They can also blackmail you.
- Never turn on your webcam while your chat partner does not connects to the webcam
- Talk to your elders or parents, if your chat partner suggests to keep your conversation with them a secret.
- Do not go to meet a person whom you met online alone. Always take a friend or an elder person with you.
- Never install unwanted Software and Apps like dating App, online games, etc. from unknown sources. You should be very careful while chatting in the chat rooms. Never share personal details in the chat room and limit your identity.

What can you do if you are a victim of cyber grooming?

If you feel that you are a victim of cyber grooming, please inform your elders so that they can intervene and support you. Following suggestions can be helpful in managing the situation.

- **Inform your parents / elders immediately:** If someone online is making you uncomfortable, you must inform your parents / elders immediately. Don't feel that your parents will restrict your online activity or ask you not to use your computer / smart phone. It is important to inform them so that they can support and guide you. Narrate the entire issue clearly to your parents/elders.

- **Block the Groomer:** If groomer is using social media platforms to groom you, you can block him/her. All the social media apps or services have the option to block a user.
- **Collect and Save messages:** Save messages, pictures or videos shared with you by the groomer. Such messages, pictures or videos can be used as an evidence to take a legal action against them.
- Your parents/elders can contact local police station to lodge a complaint against the groomer.

Do you know that producing, publishing and transmitting sexually explicit material or Child Sexual Abuse Material (CSAM) is electronic form is a punishable offense under The Information Technology Act 2000 of India?

ONLINE GAMING

Surprised how online gaming is related to cyber security? Let me tell you that more and more children and young people are gaming online and the number is going to increase many fold in future. Where ever there are lot of users on internet, cybercriminals find their way to victimize them. This can be in way of cheating, cyber bullying, sharing inappropriate content, etc.

Gaming is another area which has been transformed with the advent of information technology. More and more children are joining the online gaming community. Easy access and variety of platforms that can be used for playing online games have helped in increasing online gaming in India. Children can play online games on mobiles, consoles, computers, portable gaming devices and social networks. The gaming consoles operate like a computer where you need to create your account, login, put a headset, use web cam or other devices. You not only play games with crores of users online but also talk to them, share your views, become friends, join groups, teams, etc. There are crores of players playing online games at any given point in time. While online games can be fun, they also bring associated risks.

Do you know that you may end-up downloading spam, viruses, malicious software along with the online games that can adversely impact your computer or mobile phone or gaming console? It is important to download games from reputed sites. Never download/ install pirated games and software.

It is a matter of concern that outdoor activities and physical games are missed out on by our computer and smart phone-loving children. It is advisable to include outdoor games in addition to online games that helps you in your overall physical, mental and social development.

Given the range of online games available and ease of playing with crores of players online from across the globe, online gaming can be a fun way for you to connect with others, but it is indeed important for you to understand the associated risks and know how to handle certain situations. Enjoy the online gaming experience and have great fun, but make sure that you play it safe!!!

Do you know what are the risks associated with online gaming?

- There are many aggressive players online who may bully you. Some players play simply to bully or harass others. They may use inappropriate language or cheat others. It is important for you to be careful.
- Many adults and cyber criminals also play online games and pretend to be a child. They may try to befriend you by giving tips about the games, sharing points with you and trying to win your trust. They may use this opportunity to run a scam by

getting personal information or motivating you for a one-to-one meeting.

- There are many free online gaming websites. Moreover, you may receive links over emails or text messages to download an interesting online game. Some of the games ask lot of personal information about the player before creating an account. This may compromise your personal information like your name, age, mobile number, etc., which can be misused. You may end-up downloading viruses or malwares along with free online games downloaded from unsecure sites which can infect your computer, smart phone or other gaming devices.

- In many online games you are asked to buy points/coins, etc., which can be used to improve performance or give you advantage in terms of time or resources. You are asked to share credit card details for the payment. Of course you ask your parents to help you with the purchase. However, some infected online games can capture your credit card details and misuse it.

Concerned about online gaming? Don't worry... with awareness and precautions you can play online games safely. You need to be careful and follow safeguards to protect yourself and your friends from potential risks associated with online gaming.

Let's discuss how you can protect yourself

- Don't share your personal information like name, date of birth, address, and phone number with players while playing

online games. You don't know who the players are and what is their intention? You may end-up sharing your information with scammers or cyber bullies.

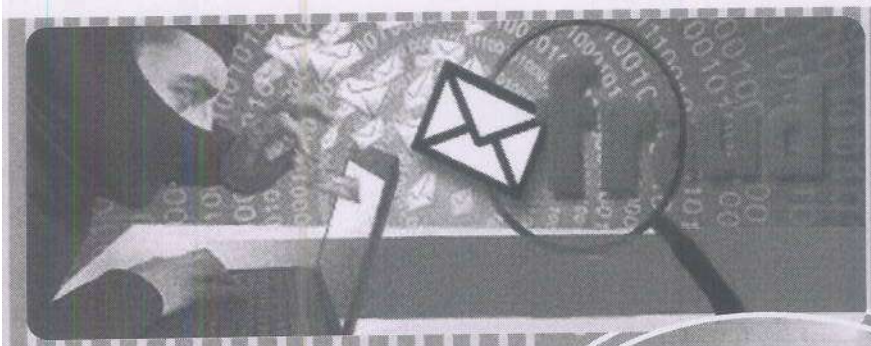
- Never share your or your parent's credit card/debit card details with anyone when you are playing online games. Some cyber criminals befriend children by helping them with winning games or sharing points. They may win your trust and later ask for your help to buy coins/points, etc. They may ask credit or debit card details. Never share such details with anyone.
- Never install games downloaded from free online gaming websites that are not reputed. Never download games by clicking on links received on mail or text message or through a popup. You may end-up downloading viruses and malwares which can compromise security of your computer or smart phone.
- Always install a good antivirus software on your computer, smartphone or other handheld devices. Regularly update the antivirus and other applications.
- Never share your passwords with anyone. You should use a complex password for your online gaming account and other online accounts. It is a good practice to change your password on regular interval.
- Never use voice chat or web cam while playing online games. This may share your identity with other players and attract cyber bullies and other cyber criminals.
- Never meet in person with someone from your online gaming world. In real life they may be very different. Cyber criminals

may befriend you and try meeting you or getting your personal information. They may have wrong intentions.

☞ If you face any challenge in online gaming world, immediately inform your parents or elders so that they can support and guide you.

Develop habit of playing outdoor games. You will enjoy outdoor activities and can make real good friends. Limit your exposure to online games as much as possible

- Do you know playing outdoor games help you in exploring the environment, developing muscle strength, gaining confidence, making new and real friends and improving your overall personality?



E-MAIL FRAUD

Most of you have your personal email account. We need an email account not just to send emails to our friends and family members but also for opening a social media account, online gaming account and other online accounts. Our email account has become an integral part of our life. As you will grow up, utility of your email account will increase. You will use your email account for connecting with bank, mobile service provider, communicate with your college, etc. It is very important to learn how to safeguard your email account

Do you know we all get unwanted mails regularly? Have you noticed Spam email box in your email account? Most of the email providers have the facility of a spam box where unwanted mails are transferred. Email fraud is very common and least expensive method used by cyber criminals to compromise other email accounts for personal gain or to cause damage to individual.

How it works?

There are many ways a cybercriminal can use an email to trigger an attack on your system or collect your important personal information. You may have heard about phishing, vishing, etc. You can read about these online but here let's try to understand in a very simple way how email frauds can happen

- A cybercriminal sitting anywhere in the world can send you an email from a fake account which looks like a genuine account. For example, you may receive a mail from your gaming portal or social media platform where spelling of service provider or email id will be slightly changed - customersupport@gammingportal.com. Have you noticed that spelling of "gaming" is incorrect? These emails contain links which would direct you to another page where you would be asked to enter passwords/ credential for technological upgrade, compliance or other fake reasons (which may sound genuine). And finally you end up giving your credentials to cybercriminals.

- Another way commonly used by cyber criminals is sending an email with a document (word or excel file) with malware (dangerous program that can impact your computer) attached to it. The title of the email or document can be very appealing to you such as tips to win famous online game or tips to receive free coins for a famous online game or any other appealing title. If you open such document the malware may get installed to your computer or mobile. This malwares could send important credentials from your computer like password, login id, etc., to the cyber criminals on regular intervals.

- Another common email fraud is when a cyber criminal sends you an email informing that you have won a lottery ora surprise gift or your distant relative overseas has left a fortune for you. The offer is so lucrative that you open the email and respond to it. The cyber criminal asks for your personal details and bank details for transferring the winning amount. They may also ask you to deposit a processing fee to enable them to transfer the winning amount. All such emails are generally fake and intention is to get your personal details or money from you. As a child you may not have bank account but you may still receive such emails. You should also share about such emails with your parents so that they can protect themselves.

- Email account hacking is another common way used by cyber criminals. They may use malware or other tricks to obtain your email id and password. Once your email account is hacked, cybercriminals can use it to get access to your critical information like social media accounts, bank accounts, etc. They can also send offensive emails to all your contacts.

- Another common trick used by cyber criminals is to hack your email and impersonating your profile and seeking financial help from all your family and friends who are in your email address book. Have you ever received an email from someone known to you asking for financial help as he or she is in emergency with limited access to phone or his/her bank account?

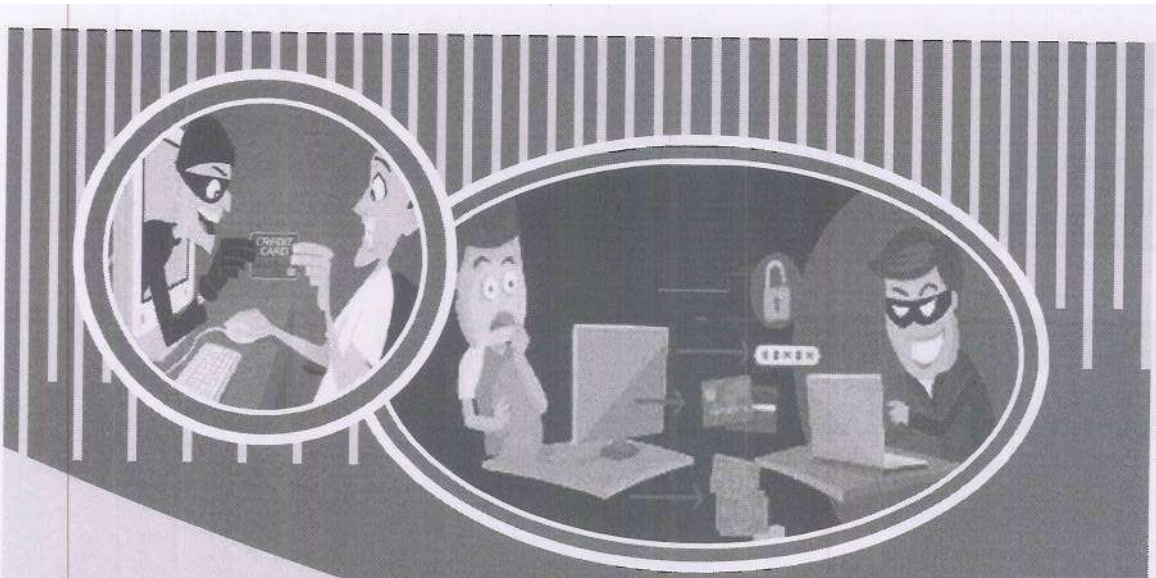
Concerned about email frauds? Don't worry... with awareness and precautions you can use email without any fear. You need to be careful and follow safeguards to protect yourself and your friends against email frauds.

Let's discuss how you can protect yourself from becoming a victim of email frauds. Don't forget to share these suggestions with your family and friends.

- First important step is to safeguard your own email id so that it is not hacked or compromised. For this, you must use a complex password and change it periodically. A simple password like Password 123 or your name or date of birth is too easy for cybercriminals to guess. Use alphanumeric combination to set a strong password.
- You can use two factor authentication for login. This feature is provided by most of the email service providers. Two factor authentication allows you to login to your account with a password plus OTP received on your mobile phone. This is a good security feature and may help you in keeping your account safe.
- Never share password of your email account with anyone. Sharing password may compromise your email account. Don't click on link or attachment from unknown sender.
- If you are using computer of your friend or a computer in a cyber café to access your email account, make sure you don't click yes on "remember password popup" which generally comes when you login from a new computer. You must never allow any computer to remember your password (this means password will not be required to login to your account on that system). Always remember to sign off from your email account after using it. Always change your password once it has been accessed from a public computer like in a cyber café.
- If you are accessing email on your mobile phone, remember to keep a strong password to access your phone.

- If your email account is hacked/compromised, send an alert email or message to all your contacts about the same and warn them not to open the links/ attachment from your email id. Immediately reach out to your email service provider through help page and request them to temporarily block your email account. Try to retrieve your password and change your password immediately.
- Never install unwanted software and apps from unknown sources. Never click on links or files received from unknown person on your email or over message. This may be an attempt to infect your computer/ phone with malware.
- If you receive an email about winning a lottery or great offer, please don't respond to it or share your personal information like name, address, bank account details, etc. If you receive an email from your service provider about an update or any other genuine reason, verify the sender's email id carefully. Check if there is any spelling mistake. Avoid clicking on links from such emails. Try to connect with service provider to check if the email is genuine.
- If you receive an emergency email from your friend or relative asking for financial help, try to connect with that person over phone or through other known people to validate the authenticity of the email. There may be a possibility that his or her account has been hacked and used to send such email.
- Be watchful and develop a habit to change passwords at regular intervals, ignore emails from unknown sources, and restrict yourself from sharing personal details on email and clicking links/documents received from unknown sources.

Do you know cheating people using communication devices or otherwise is a punishable offence



Online Transaction Fraud

Though most of you may not be using banking services such as debit card, credit card, net banking, etc., at this stage but as you grow up you may start using these services. Moreover, as a smart citizen you must understand how online transaction frauds can happen so that you can teach other's in your family and friend circle.

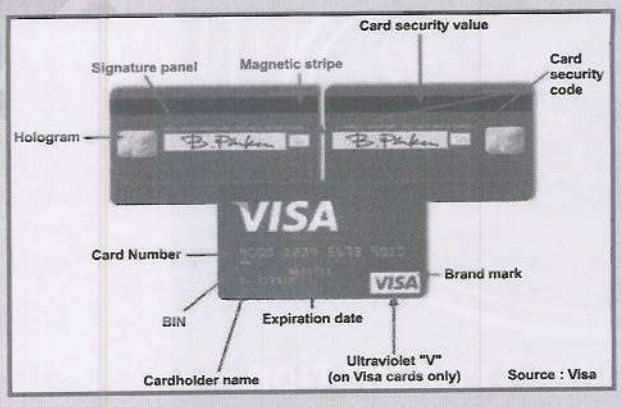
Online transaction fraud means illegally withdrawing or transferring money from your account to another account by a cyber criminal. Online transaction frauds can happen when your login credentials or bank account details or credit card details are stolen by a cyber criminal.

How it works?

There are many ways used by cybercriminals to cheat people online.

Cyber criminals can send an email to you from a fake account which appears to be from your bank or credit card service provider. When you click on link provided in the email it takes you to a page

where your sensitive information like bank account details, card details, card verification value (CVV), expiry date, etc., is asked. Once you share these details, your account can be compromised.



Cyberc riminals may fake his/her identity and call you posing as a bank employee and try to obtain credit card or bank details such as account number, personal identification number (PIN), CVV, expiry date, date of birth, etc. Once such details are given, the account can be compromised.

Do you know your debit/credit card PIN is unique number which is required to access your card on ATM or for other online transactions? You can change your PIN number easily. It is a good practice to change your PIN periodically.

Usually, our mobile number is linked with our bank account. Cyber criminals may also call you, posing as an employee of mobile service provider and inform you that your mobile number will be disconnected if you don't update your Subscriber Identification Module (SIM). For updating the SIM, they will send you a link or ask you to send an SMS from your number to service provider. Actually, they are attempting to make you send an SMS to your mobile service provider to block the existing SIM and issue a

duplicate SIM. They obtain the duplicate SIM from service provide and use it to transact online using your mobile number and banking app.

Do you know that bank would bear the loss of banking frauds only if negligence or security laps is found at bank's end?

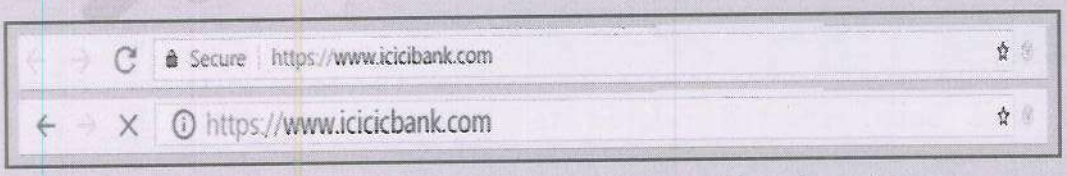
Total 1785 cases have been reported related to credit/debit card and Internet banking fraud in the year 2017 alone. This amounted to a total loss of R.s 71.48 crores.

Concerned about online transaction frauds? Don't worry...with awareness and precautions you can safeguard yourself against online transaction frauds. Please remember if you don't share your bank and card details like card number, PIN, CVV, expiry date,bank account password, etc., with anyone, you may be able to protect yourself against online transaction frauds. You need to be careful and follow safeguards to protect yourself and your friends against such frauds.

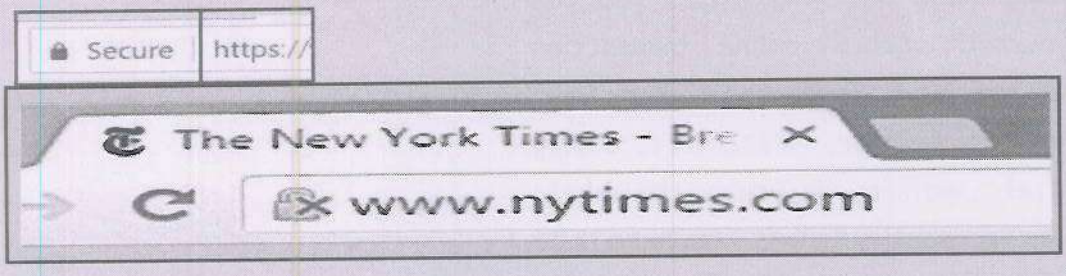
Let's discuss how you can protect yourself from becoming a victim of online transaction frauds. Don't forget to share these suggestions with your family and friends.

- Never share your bank and card details such as online account password, card number, CVV, expiry date, PIN, OTP, etc., with anyone. By sharing these details you will compromise your account which can lead to illegal online financial transactions.
- Make it a habit to regularly update your online password of your bank account and PIN of your Debit/Credit cards.
- Always make it a habit to type bank website yourself when

trying to login to your bank account. You must not click on a link of bank website appearing on an email, text message or a popup. This may be a fake link and may take you to a fake site. Once you login to your bank account from a fake site, your sensitive details like account number and password may be stolen.



☞ Check for the bank's security certificate details and various signs such as green address line, lock sign on the address bar and HTTPS to confirm you are visiting a secure bank website

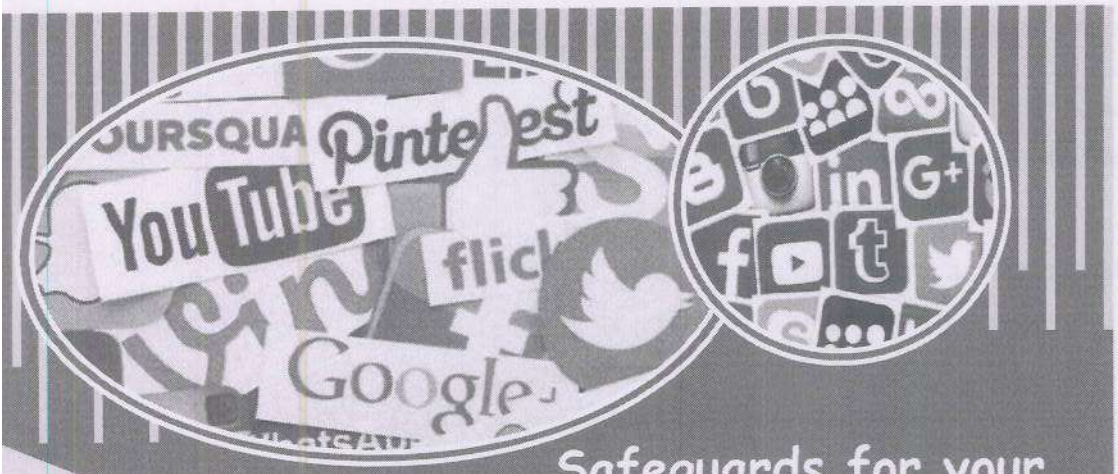


☞ Always check the website URL starts with HTTPS. The website URL with HTTPS encrypts your data in the website and protects it from any kind of tampering. Do not share your confidential information such as online account password, card number, CVV, expiry date, PIN, OTP, etc. on the website which doesn't start with HTTPS.

☞ It is equally important to protect your mobile phone as your mobile number is linked with your bank account. Always use a strong password to open your mobile phone and install a good antivirus software. If you receive a call from mobile service provider informing you that your number will be deactivated if you don't update it or any other such message, please be

cautious. Disconnect the phone and call customer care number of your mobile service provider to check if the call was genuine.

- Never install pirated software on your mobile or computer. It is not only illegal but may also compromise security of your devices. Always install a good antivirus on your computer and mobile phone. It is important to keep your computer software and anti-virus up-to-date.
- Avoid making online transactions using a public Wi-Fi or a computer in a cyber café. Computers in the cyber café may not have updated antivirus or may be infected with malware which may compromise your bank details and other sensitive information such as card number, expiry date, CVV, etc.
- Make it a habit to review the monthly statements of your bank account and credit cards. Check if there is any unrecognized transaction.
- If you find that your bank account or card details are compromised/stolen by someone or your debit or credit card is lost, call the bank immediately and block your card/account immediately. If unauthorized transactions have taken place, you must lodge a formal complaint at your nearest police station.



Safeguards for your social networking profiles

Social networking sites such as Facebook,Twitter, Instagram, Snapchat, etc., are extensively used by all of us. We love sharing an update or a selfie or pictures with our friends and relatives. We love receiving likes and comments on our posts/pictures and updates. While social networking sites have helped us in connecting with our friends and relatives easily, there are serious cyber threats that can impact us if we are not careful.

How it works?

Cyber criminals and cyber bullies can use social networking platforms to harm us. Let us learn about common cyber threats related to social networking sites which can impact anyone of us.

- Cyber criminal can create your fake account on social media and use it to share negative things and inappropriate content to harm your image or for other illegal purposes. This is a very real threat and can impact anyone. It is easy to create a social media account using any email id. These days our pictures, email id, date of birth and other details are easily available online. Cyber criminals can use these details to create our fake account.

- Cyber bullying is very common on social media platforms. Cyber bullies can use social media to send rude or hurtful messages to demean or hurt you.
- Online frauds can be triggered through links shared on social networking sites. Cyber criminals share a post with a malicious link or a malware. If you click on the link, your computer or mobile can be infected or compromised.

Concerned about cyber threats on social networking platforms? Don't worry... with awareness and precautions you can safeguard yourself and use social networking sites safely. You need to be careful and follow safeguards to protect yourself and your friends against such frauds.

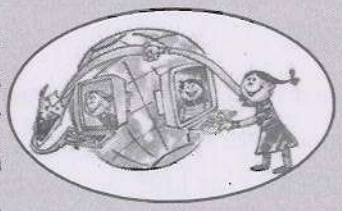
Let's discuss how you can protect yourself and your social media accounts. Don't forget to share these suggestions with your family and friends.

- First important step is to safeguard your own social networking account so that it is not hacked or compromised. For this you must use a complex password and change it periodically.

Do you know that most of the social media sites and email service providers give you an option of two factor authentication to login in to your account? You can go to settings and activate two factor authentication. This means you will need to type your password and One Time Password (OTP) received on your mobile to login to your account. It is a good safety feature and should be used for all your accounts.

- Never share password of your social media account with anyone. Sharing password may compromise your account.
- Whatever you post on social networking sites can be visible to everyone unless you restrict the access of your posts to your friends/followers. You must change the privacy settings of

your social media account and ensure that your updates/posts, etc. are visible to your friends/followers only.



- Avoid accepting friend request from unknown people. Before accepting a friend request try to see how many other people are following or are in friend's list of the requestor. Cybercriminals can create fake account of your known person so be careful.
- Whatever you post on social media generally remains there. Be careful before posting anything on social media. Think if the information can be shared with everyone. Never share your personal details such as address, phone number, date of birth, etc. on social media sites.
- If you are using computer of your friend or a computer in a cyber café to access your social media accounts, make sure you don't click yes on "remember password popup" which generally comes when you login from a new computer. You must never allow any computer to remember your password (this means password will not be required to login to your account on that system). Always remember to sign off from your account after using it.
- If you are accessing social media accounts on your mobile phone,remember to keep a strong password to access your phone.
- If your social media account is hacked/compromised, send an alert email or message to all your contacts. Immediately ask your social media service provider to temporarily block your account. Try to retrieve your password and change your password immediately.
- If you notice that your fake account has been created, you can immediately inform social media service provider so that the account can be blocked. If someone is bullying you, posting inappropriate comments or images or creating your fake account to damage your image, inform your parents or elders

immediately so that they can support and guide you. With support from your parents, you can also register a complaint at your nearest police station.

- Never install unwanted software and apps from unknown sources. Never click on links or files received from unknown person on social media. This may be an attempt to infect your computer with a malware.
- Fake news or Hoax messages spread like wildfire on social media. It may create law and order problem and may end-up causing loss of life in few cases. Before forwarding or sharing any message on social media or messaging app, check it on other sources also to confirm its authenticity.
- Never download or upload copyrighted content such aspoems, essays, videos, music, images, composition of songs, music, software, etc. without the author's permission. The act of downloading and uploading copyrighted work of others is an offence.

Hope you enjoyed reading this handbook. These suggestions should help you in protecting yourself from cybercrimes. As you know cybercriminals frequently devise new ways to cheat people. It is important to remain up to date with new threats and ways to protect ourselves.

Few suggestions from your CyberDost

- Read more about cybersecurity, emerging new threats and ways to safeguard against cybercrimes.
- Be a good cyber citizen. Use precautions yourself and educate your friends and family about cyber security
- You can follow us on twitter handle @ Cyber Dost for regular updates on safe cyber practices.
- We request you to please share your feedback with us on dircis2-mha@nic.in or pmuiec.cis-mha@nic.in

YOUR CYBER DOST

Ministry of Home Affairs
Government of India