GOVERNMENT OF ASSAM
OFFICE OF THE **DIRECTOR OF HIGHER EDUCATION**, ASSAM,
KAHILIPARA, GUWAHATI-19.
****

No. DHE/CE/Misc.95/2018/22 Dated Kahilipara, the 29-03-2019

From:- Smti. Gitimoni Phukan, *A.C.S.*
Director of Higher Education, Assam
Kahilipara, Guwahati-19.

To,

The Principal (All),
Govt./Provincialised Colleges of Assam.

Sub: Regarding creating awareness amongst children/adolescent with regard to cyber crime and its related safety for protecting themselve.

Ref: *Govt. letter No. AHE.529/2017/152, dated 21-02-2019.*

Sir,

With reference to the Govt. letter on the subject cited above, I would like to forward herewith Govt. letter No. AHE.529/2017/152, dated 21-02-2019, regarding creating awareness amongst children/adolescent with regard to cyber crime and its related safety for protecting themselve for favour of kind information and necessary action from your end.

Yours faithfully

30/3/19

Director of Higher Education, Assam
Kahilipara, Guwahati-19.

Memo No. DHE/CE/Misc.95/2018/22-A Dated Kahilipara, the 29-03-2019

Copy to:-

1) The Joint Secretary to the Govt. of Assam, Higher Education Department, Dispur, Guwahati-6 for information.

Director of Higher Education, Assam
Kahilipara, Guwahati-19.

GOVERNMENT OF ASSAM
HIGHER EDUCATION DEPARTMENT
ASSAM SECRETARIAT:::BLOCK'C' GROUND FLOOR
DISPUR:::GUWAHATI-6
email: higherednassam@gmail.com

No. AHE. 529/2017/152 Dated Dispur, the 21st February, 2019

From : Smti N.Laskar,ACS
Joint Secretary to the Govt of Assam
Higher Education Department.

To : 1) The Director of Higher Education,Assam
Kahilipara, Guwahati-19

2) The Director of Technical Education,Assam
Kahilipara, Guwahati-19

Sub. : Regarding creating awareness amongst children/adolescent with regard to cyber crime and its related saftey for protecting themeselve.

Madam,

With reference to the subject cited above, I am directed to enclose herewith the copy of letter No.PLA.256/2017/46 dtd. 4/01/2019 received from Secretary,Home and Political deptt. and requesting to put the information in the website.

Enclo-As stated.

Yours faithfully,

Joint Secretary to the Govt. of Assam
Higher Education Department.

Memo No. AHE. 529/2017/152-A Dated Dispur, the 21st February, 2019

Copy to:

1) B.R. Sharma,Special Secretary,Ministry of Home Affairs,Govt. Of India,North Block,New Delhi-110001

By order etc.,

Sd/-

Joint Secretary to the Govt. of Assam
Higher Education Department.

YOUR CYBER DOST

सत्यमेव जयते

Ministry of Home Affairs
Government of India

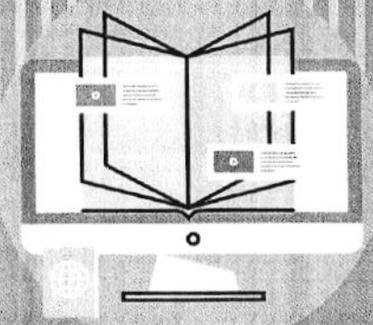
This booklet has been prepared in consultation with Cyber Security experts.

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.

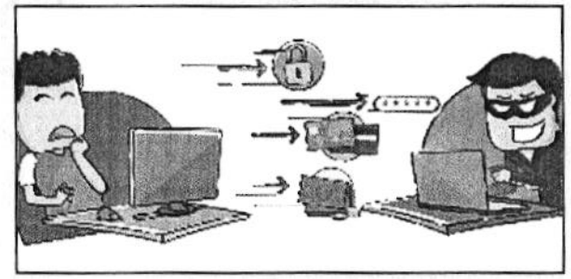
WHY IS CYBER SECURITY A CONCERN?

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?

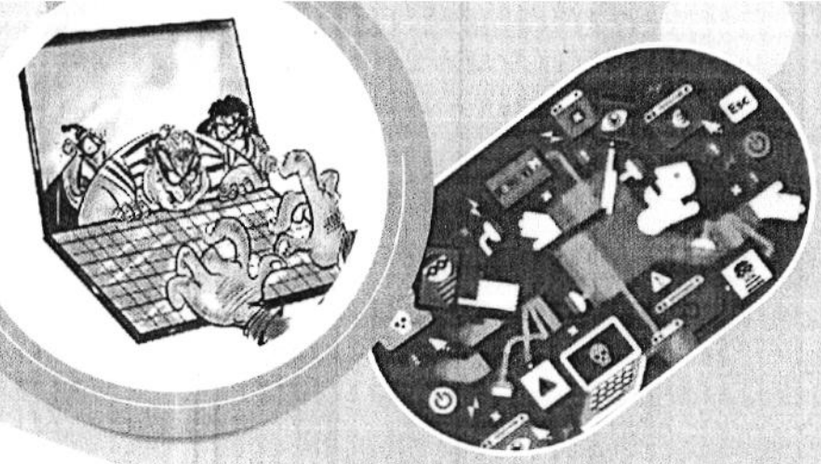
Cybercrimes are offences that may be committed against individuals, companies or institutions by using computers, internet or mobile technology. Cybercriminals use platforms such as social networking sites, emails, chatrooms, pirated software, websites, etc., to attack victims. Children are also vulnerable 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.

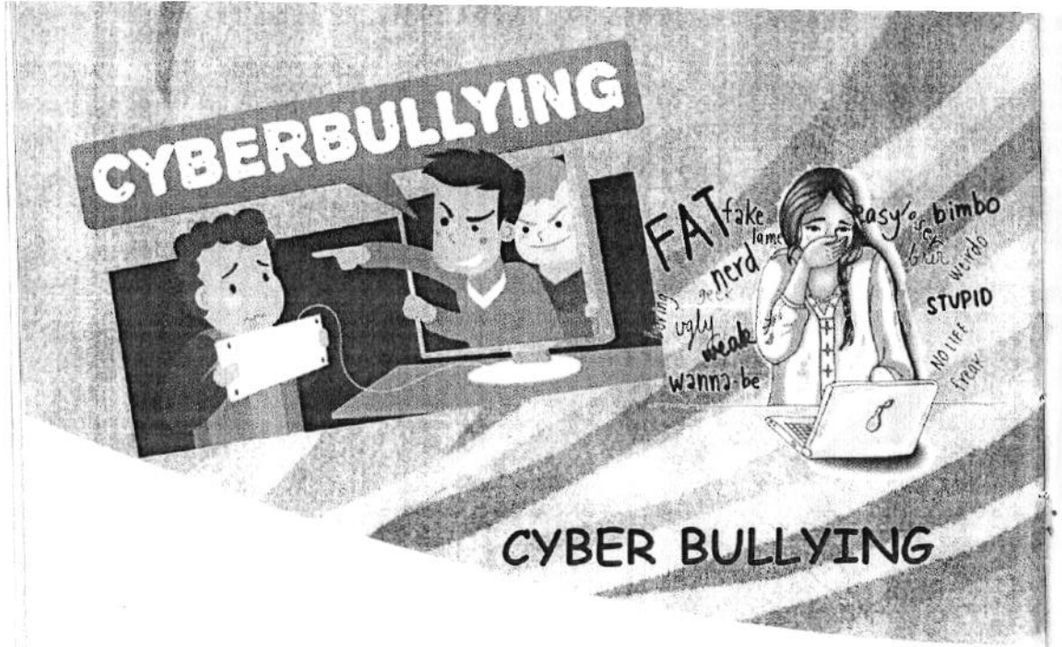
Do you know a hacker is anyone who uses/ exploits technology for an unintended use thereby disrupting operations or causing financial/ reputational lossto people? Hackers can use malwares, viruses or Trojans to attack your computer and gain access to your data.

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

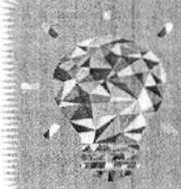
- If your parents/elders feel the need, they can contact local police station to lodge a complaint against the bully

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.

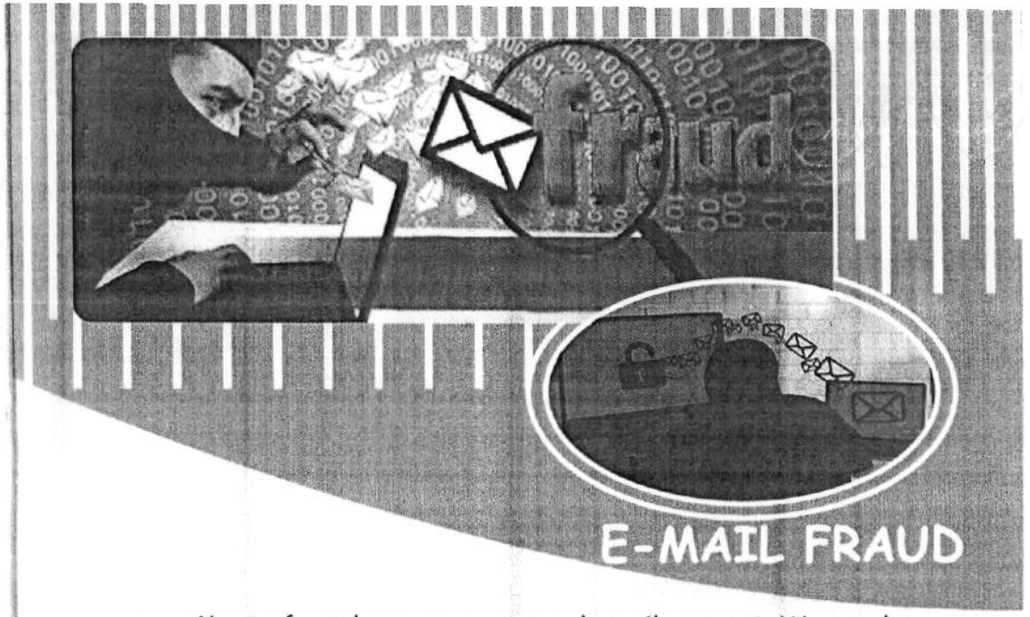
may befriend you and try meeting you or getting your personal information. They may have wrong intentions.

- 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.

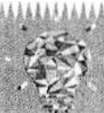
- If your email account is hacked/compromised, send an alert email or message to all your contacts about the same and warn them not to open the links/ attachment from your email id. Immediately reach out to your email service provider through help page and request them to temporarily block your email 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.

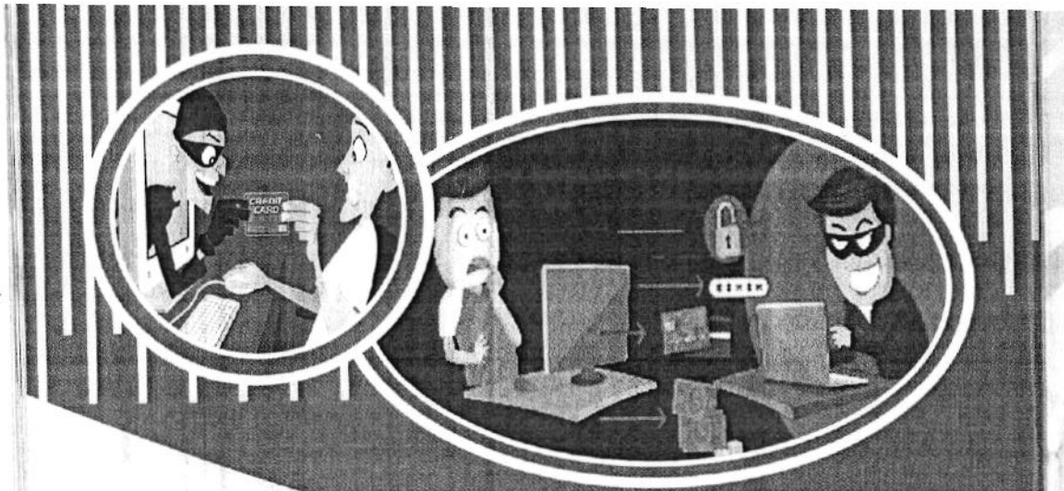
- If you receive an email about winning a lottery or great offer, please don't respond to it or share your personal information like name, address, bank account details, etc. If you receive an email from your service provider about an update or any other genuine reason, verify the sender's email id carefully. 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.

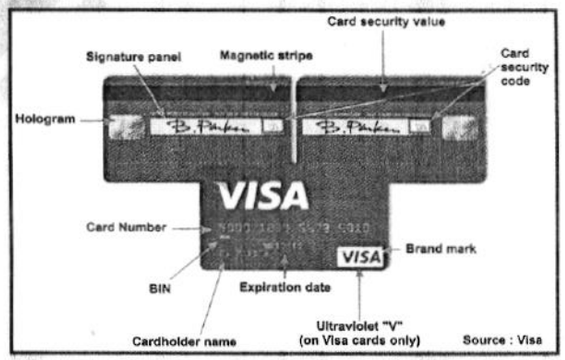
Online transaction fraud means illegally withdrawing or transferring money from your account to another account by a cyber criminal. Online transaction frauds can happen when your login credentials or bank account details or credit card details are stolen by a cyber criminal.

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