Guidelines for cyber safety of children

With the increasing use of technology these days it is very important to educate children about cyber safety. Cyber criminals use platforms such as social networking sites, emails, chatrooms, pirated software, websites, online games etc., to attack victims. Children are more vulnerable to these cybercrimes.

1. **Cyber Security one of the prime concern**
   a. Information or personal details shared on internet stay online forever, which can be used by cyber criminals for creating fake profiles, cyber bullying etc.
   b. There are many types of cyber threats like **Spam emails, Banking frauds, Cyber bullying, Identity theft, Getting access to your computer/ smart phone, Job frauds and cyber grooming etc**.
   c. Many adults and cyber criminals pretend to be children and may try to befriend by giving tips about games, sharing points etc. to win the children's trust.
   d. Sometimes strangers build an emotional bond with children/ teenagers through social media or messaging platforms with an objective of gaining their trust for sexually abusing or exploiting them.
   e. There are not only physical, emotional, psychological consequences of cyber bullying on children but it also impacts their academic performance and daily life.

2. **Tips for students to save themselves from becoming a victim of cybercrime**
   a. Don't accept friend request from unknown people on social media platforms
   b. Don't share your personal information like date of birth, address and phone number on social media or other platforms.
   c. Never share your parent's credit/debit card details with anyone.
   d. Restrict access of your profile to your friends only by applying privacy settings to your accounts.
   e. Remember what you post online remains forever so be careful while sharing your details/ pics/ videos etc.
   f. Never install unwanted software and apps like dating app, online game, pirated software etc. from unknown sources.
   g. Always install a good antivirus software on your computer. Smartphone and regularly update it.
   h. Don't give your personal details while downloading a game/ software.
   i. Never share your passwords with anyone. Also it is a good practice to change your passwords on regular interval.
   j. Never answer unknown / spam emails.
   k. Avoid chatting with people who ask you questions related to your physical or sexual experiences.
   l. Never turn on your webcam while playing online games or while your chat partner does not connect to the webcam.
   m. Do not go alone to meet a person whom you met online.

3. If you are a victim of cyber bullying
   a. **Seek help from your parents/ elders** immediately to reach out to the bully.
   b. **Block the bully** from all the social media platforms.
   c. **Save posts/ messages** as they can be used as an evidence, in case of legal action has to be taken.
   d. If your parents/ elders feel the need, they can contact the local police station to lodge a complaint against the bully.

4. **Safeguarding your email account** - 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.
    a. A cybercriminal sitting anywhere in the world can send you email from a fake account which looks like a genuine account.
    b. Another way commonly used by cyber criminals is sending an email with a document with malware(a dangerous programme that can harm your computer). The malwares could also send important credentials from your computer like passwords, login id, etc. to cybercriminals on regular intervals.
    c. Another common fraud is when cyber criminals send you an email giving lucrative offers or informing that you have won a lottery or gift.
    d. Email account hacking is very common, once your account is hacked, cyber criminals 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.
    e. Tips to protect from being a victim of email frauds:
        i. Use complex password and change it periodically.
        ii. Two factor authentication can be used for login which allows you to login to your account with a password plus OTP received on your mobile phone.
        iii. Never share your password with anyone.
        iv. Don’t click on the link or attachment from unknown sender.
        v. Never click yes on “remember your password popup” while working on any other computer than your own.
        vi. Always remember to sign out from your email account after using it.
        vii. If your account is hacked send an alert email to all your contacts to warn them about the same.
        viii. Never respond to any lucrative offer like winning a lottery or great offer.
5. **Online Transaction Fraud** is illegally withdrawing or transferring money from your account to another account. Tips to protect yourself from becoming a victim of this.
    a. Never share your bank or card details such as online account password, card number, CVV, expiry date, PIN, OTP, etc., with anyone.
    b. Regularly update your online password of bank account and PIN of your debit/credit card.
    c. Always type bank website name yourself while trying to login to your bank account. This may be a fake link and may take you to a fake site.
    d. 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
    e. 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.
    f. It is equally important to protect your mobile phone as mobile number is linked with your bank account.
    g. Avoid making online transactions using a public Wi-Fi or a computer in a cyber café.
    h. 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.