

Types of Cyber Crime & Awareness





Cyber Bullying

Aa Bb Cc Dd Ee Ff Gg Hh

“Cyberbullying is the use of inappropriate behaviour, strength or influence, whether directly or indirectly, and whether verbal, written, physical or through displays of or use of imagery, symbols or otherwise, to intimidate, torment, threaten, harass or embarrass others, using the Internet or other technology, such as mobile telephones.”



- Harassment
- Outing
- Cyberstalking
- Fraping
- Fake Profiles
- Dissing
- Trickery
- Trolling
- Catfishing



Harassment

Harassment is a sustained, constant and intentional form of bullying comprising abusive or threatening messages sent to your child or to a group. This is a very dangerous form of cyberbullying. It can have serious implications for your child's wellbeing.



Outing

Outing is a deliberate act to embarrass or publicly humiliate your child or a group through the online posting of sensitive, private or embarrassing information without their consent. Even reading out your child's saved messages on their mobile phone can be considered a form of outing.

Personal information should not be shared



Cyberstalking

This form of cyberbullying can extend to the cyberbully making real threats to your child's physical wellbeing and/or safety. Cyberstalking can also refer to the practice of adults using the Internet to contact and attempt to meet with young people for sexual purposes. It is a very dangerous form of cyberbullying and can have serious consequences if something isn't done immediately to stop it.



Fraping

- Fraping is when somebody logs into your social networking account and impersonates your child by posting inappropriate content in their name.
- Impersonating somebody online and ruining their reputation can have serious consequences.



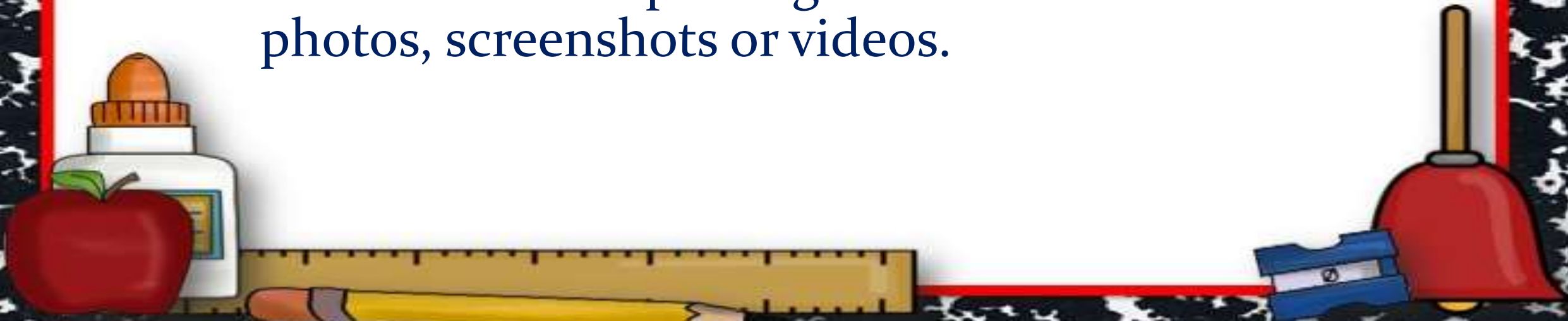
Fake Profiles

Fake profiles can be created in order for a person to hide their real identity with the intention of cyberbullying your child.



Dissing

Dissing is the act of sending or posting cruel information about your child online, to damage their reputation or friendships with others. It can also include posting material online such as photos, screenshots or videos.



Trickery

Trickery is the act of gaining your child's trust so that they reveal secrets or embarrassing information that the cyberbully then shares publicly online.



Trolling

Trolling is the deliberate act of provoking a response through the use of insults or bad language on online forums and social networking sites. The troll will personally attack your child and put them down.



Catfishing

- Catfishing is when another person steals your child's online identity, usually photos, and re-creates social networking profiles for deceptive purposes.
- A catfish is someone who wants to hide who they are. They will look at your child's social networking profile and take any information they want to create a fake persona.





Role of Parents & Teacher

- Specify clear rules, Guidelines and policies regarding the use of the Internet.
- Teach students that all types of bullying are unacceptable and are subject to discipline.
- Mentoring the students and establishment of peer monitoring.
- Use Desktop Firewalls, Browser Filters to avoid or prevent children from cyber bullying or accessing inappropriate content. Use monitoring along with software tools for students online activity.
- Educate students by conducting various workshops by an internal or external expert to discuss related issues in cyber bullying.

Sextortion





Sexting

Sexting involves the sending of a sexual message and/or revealing photos to another person. Many girls have sent nude photos of themselves to their boyfriends. When they break up, the boyfriend has sent the picture to kids at school. In some extreme cases, girls have committed suicide in these situations.



Sextortion

- Sextortion is defined as blackmail in which sexual information or images [sexting] are used to extort sexual favours and/or money from the victim.
- Social media and text messages are often the source of the sexual material and the threatened means of sharing it with others.



Role of Teacher / Parents

- Kids should be encouraged to report any nude pictures they receive on their cell phone to a trusted adult.
- The message should not be deleted. Instead, parents, guardians, teachers, and school counselors should be involved immediately.

Cyber Stalking



- Stalking generally means a harassing behavior which one person exhibits towards the other.
- Stalking may comprise of following a person, appearing at a person's home or place of business, making harassing phone calls, leaving written messages or objects.



- Cyber stalking that starts and continues on the internet and comprises of threatening victims on the internet, sending harassing e-mail or morphed photographs of the victim being displayed on pornographic websites.
- Cyber stalking that begins online and then spreads in the real world when the perpetrator finds out about the personal details of the victim and persistently follows the victim and may indulge into sinister behavior like giving death threats and causing physical assault to the victim.





Legal Definition of Stalking

Sec. 354D IPC:-

Any man who—

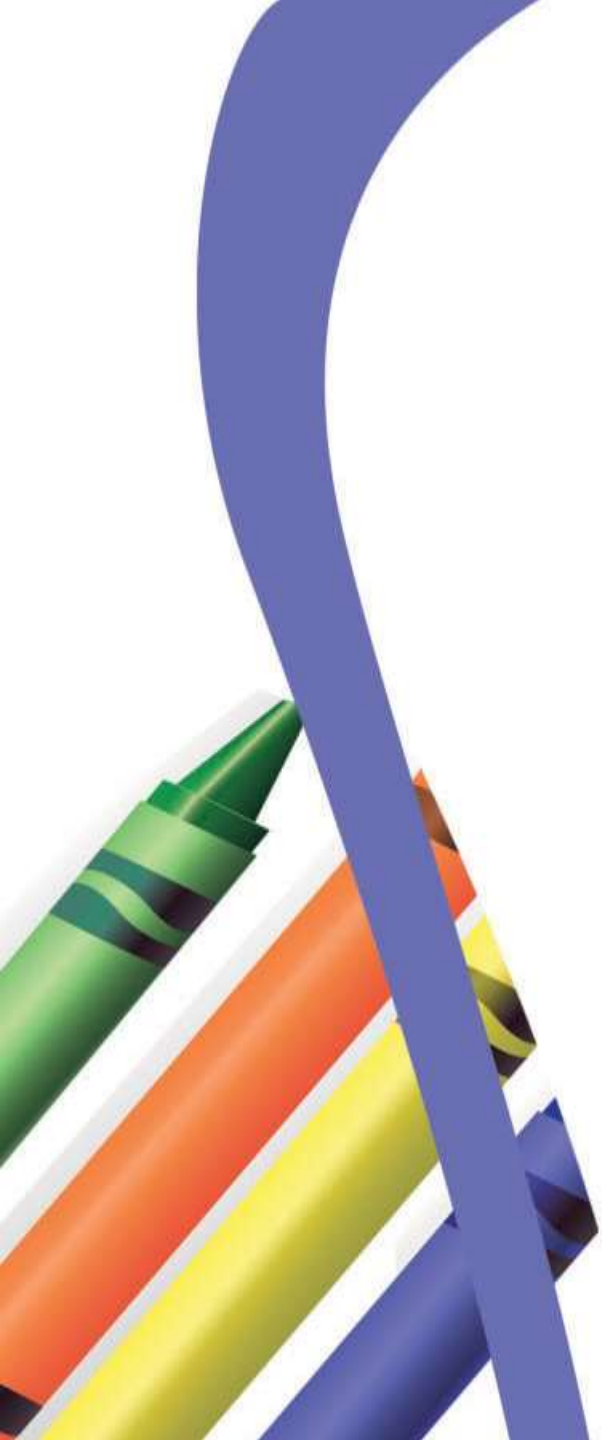
- follows a woman and contacts, or attempts to contact such woman to foster personal interaction repeatedly despite a clear indication of disinterest by such woman; or
- monitors the use by a woman of the internet, email or any other form of electronic communication, commits the offence of stalking





Pornography



- 
- Pornography is posting, publishing, and transmitting obscene messages, photographs, videos, and text thorough e-mail, websites, chatting, and other forms over the Internet.
 - Child pornography is one of the biggest ventures on the Internet.

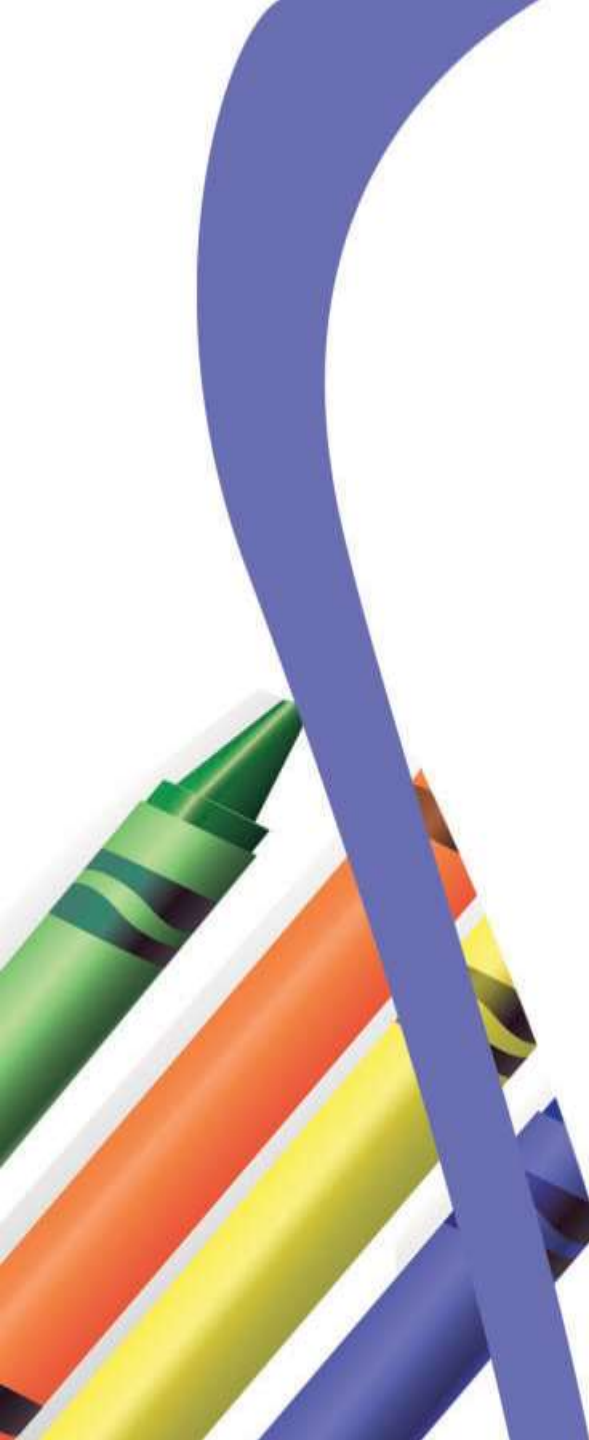
Identity Theft



A decorative graphic on the left side of the slide. It features four colored pencils (green, orange, yellow, and purple) arranged diagonally. A thick, curved purple ribbon or line arches over the pencils, extending from the top left towards the bottom right.

It is the theft of sensitive identity information:-

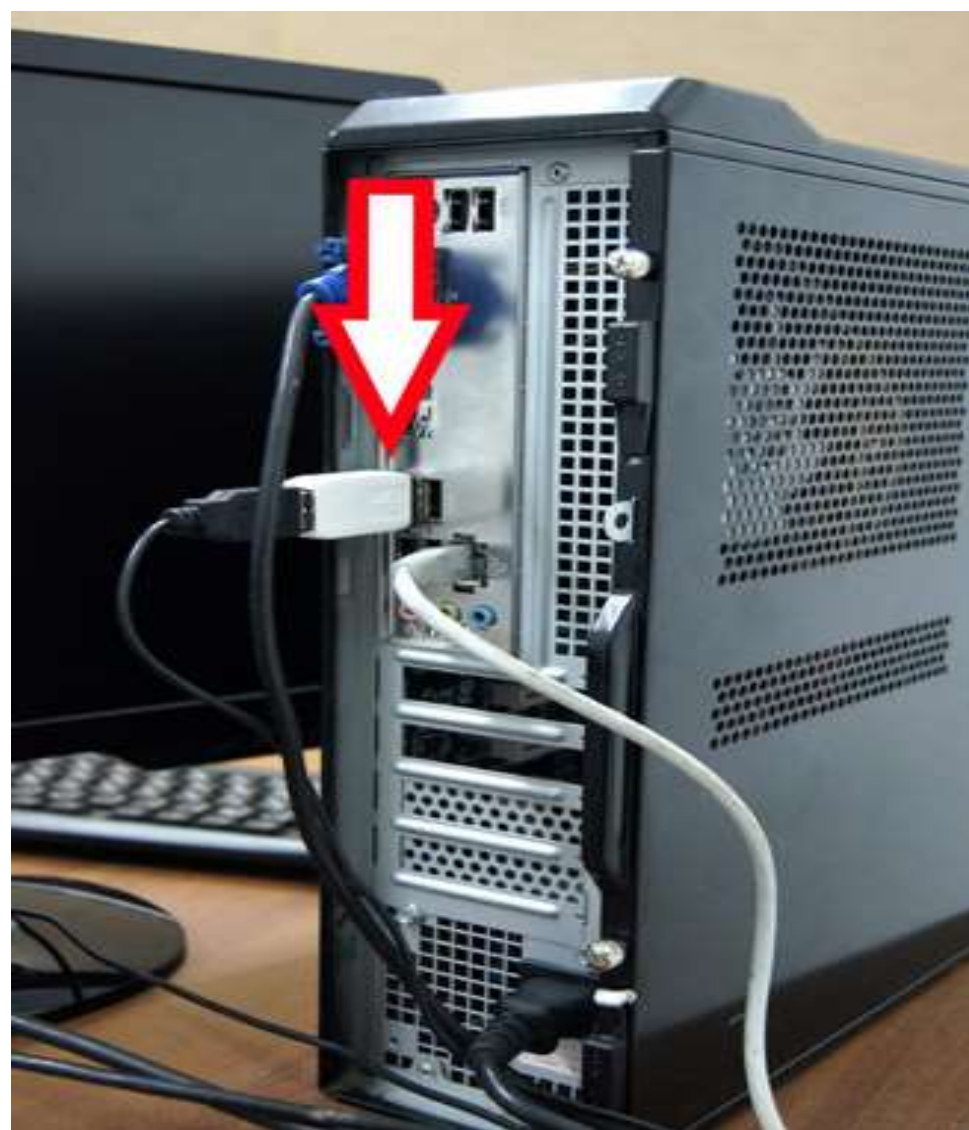
- 1. date of birth,**
- 2. name,**
- 3. PAN numbers,**
- 4. passport numbers,**
- 5. credit card numbers,**
- 6. e-mail accounts, etc.,**

A decorative graphic on the left side of the slide. It features four colored pencils (green, orange, yellow, and blue) arranged diagonally. A thick, light blue ribbon or line curves around the pencils, starting from the top left and extending towards the bottom right.

Use the sensitive information for fraudulent purposes. The user may obtain the sensitive information by several means like phishing, sending some links to victim's e-mail address and asking them to furnish confidential information, or obtaining the information through social engineering, using key-loggers, etc.

Be careful about Key Loggers at
Cyber Cafes. It is designed to
secretly monitor and log all
keystrokes





Features of ATM Card

16 digits ATM Card Number

Expiry date of ATM Card

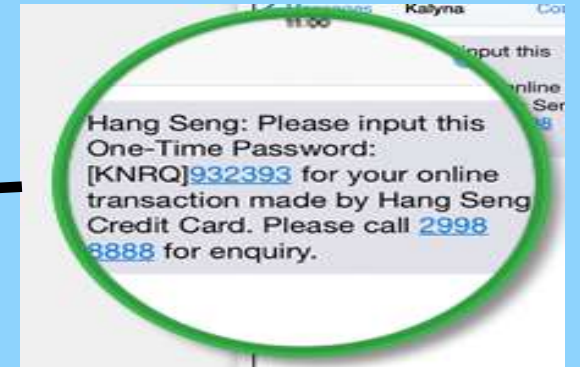
Card Holder's name

CVV Number written at the back
side of ATM Card



ONE TIME PASSWORD (OTP)

One Time Password (OTP)



- Read carefully the messages received from the Bank.
- Don't share 06 digits OTP received in your mobile phone with anyone.
- If you are unable to understand the content of SMS, then clarify from the Bank Officials.





ATM MACHINE



→ ATM Display Screen

→ Card Reader

→ ATM Keypad

→ Cash Dispenser

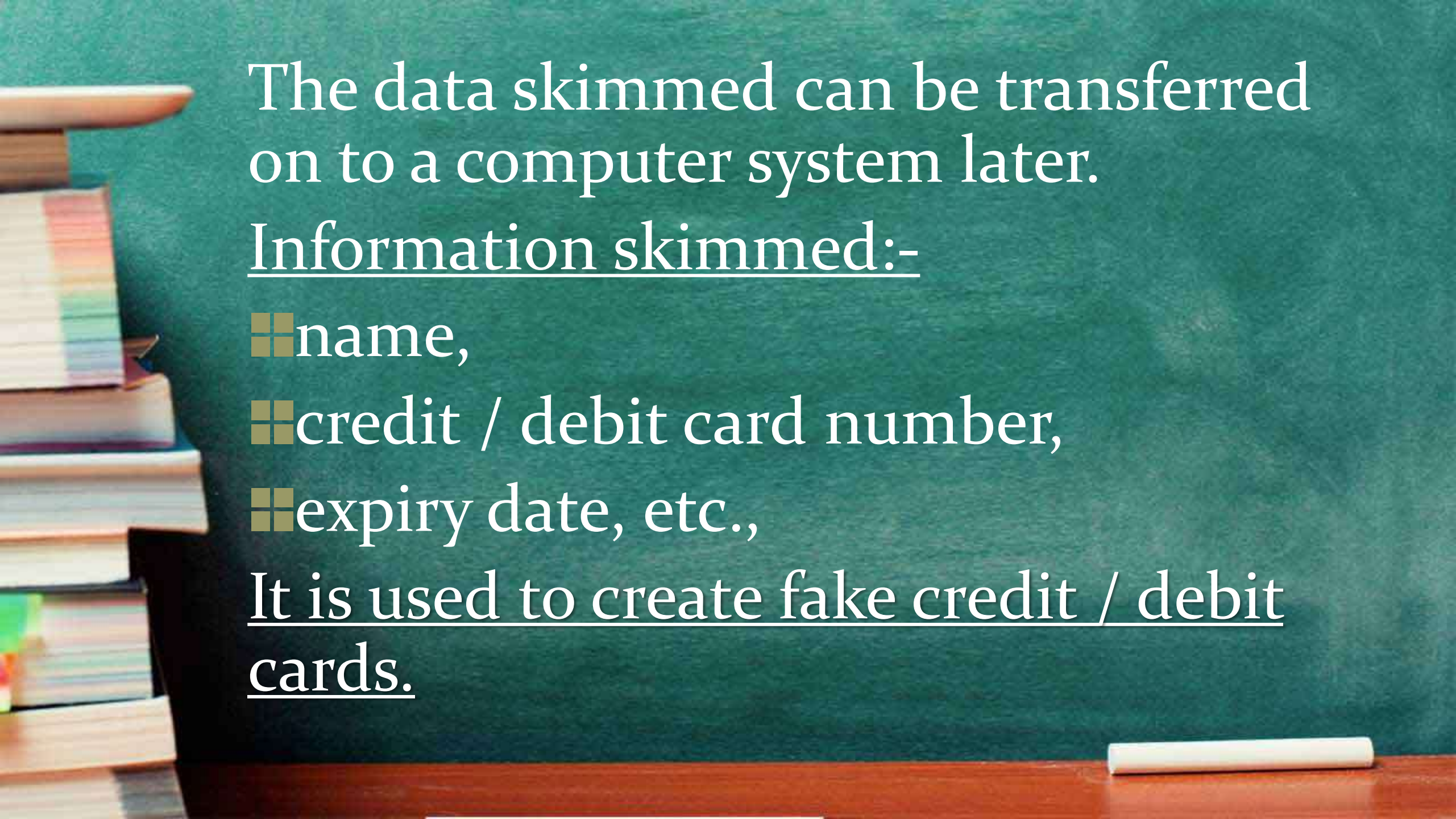
Skimming

Skimming is a kind of:-

- ✦ Credit card fraud
- ✦ Debit card fraud
- ✦ Chip card fraud

Skimmer is used to capture the information contained in it





The data skimmed can be transferred on to a computer system later.

Information skimmed:-

- name,
- credit / debit card number,
- expiry date, etc.,

It is used to create fake credit / debit cards.







A decorative graphic on the left side of the slide features a thick, wavy blue ribbon that curves upwards. Below the ribbon, several colored pencils are visible, including green, orange, yellow, and blue ones, arranged diagonally.

Precautions at ATM Booth

- Don't give ATM Card to anyone.
- Remember your ATM PIN (Personal Identification) number.
- Don't write PIN Number on ATM Card.
- Don't take the help of outsiders at ATM Booth.



Precautions at ATM Booth

- Check for the Skimmer at ATM Booth around Card Reader Slot area.
- Change your ATM PIN Number at regular intervals.
- **Link your mobile phone number with the Bank Account**

Don't allow Outsiders at the time of withdrawal of money



**Keep a strict vigil on the movement of outsiders
and cover your hand as you enter your PIN**



Precautions at ATM Booth



A decorative graphic on the left side of the slide features a thick, curved blue ribbon and several colored pencils in green, orange, yellow, and blue, arranged diagonally.

Types of ATM Fraud

- **Exchange of ATM Card / Card Theft**
- **Card Skimming**
- **Card Trapping**
- **VISHING**
- **ATM malware/ cash out attack/ jackpotting**
- **Keypad jamming**

Vishing





- Fraudsters will pretend themselves as ATM Relations Manager calling from Mumbai & Delhi Head Office and will inform you regarding blocking of your ATM card operation **or** Your ATM Card will be linked with Aadhar Card **or** Your ATM Card will be updated.
- Fraudsters will instruct you to furnish the 16 digits ATM Card number, validity of ATM Card & CVV number written at the back side of the card.





- After furnishing of 16 digits ATM Card number, validity of ATM Card & CVV number written at the back side of the card, 06 digits OTP (One Time Password) number will be delivered to your registered mobile phone number and fraudster will ask for the said OTP number.
- After furnishing of those information; online fraudulent transaction will be made by the accused.





- This type of fraud is termed as Vishing Fraud.
- Please don't share your bank related information to anyone.
- As per Reserve Bank of India Guidelines, no Bank or Insurance Company will ask for banking related information from the Customer through phone or e-mail.



Stay Safe on Social Media

- Don't post personal details, such as your phone number, home address, full name or date of birth or any banking credentials
- Read the site's privacy policy and use its privacy and security settings to control who can see your personal information.
- Don't make your profile public. Use settings so that only friends can view your full profile.
- Use strong passwords. Make it at least eight digits long and a combination of upper and lower case letters, numbers and symbols. Eg; Ps@2d#Er&
- Use a separate password for each social account.
- Don't share your password with anyone.



Stay Safe on Social Media

- Don't accept every friend or follower request you get . only connect with people you know in real life or whose identity you know is genuine.
- Never give details of upcoming holidays nor post holiday snaps while you're away. Criminals scour social networks to find empty houses to burgle.
- Don't believe everything you read online. People may post false or misleading information about various topics, including their own identities.
- Install software updates so that attackers cannot take advantage of known problems or vulnerabilities.



Stay Safe on Social Media

- Login through genuine homepage of Facebook i.e., <https://www.facebook.com>
- Avoid clicking on links in messages, tweets, posts, and online advertising. These may be links to viruses or other forms of malicious content.
- Disable location services on Facebook, Instagram, Twitter, etc. when posting photos.
- Protect your computer by installing antivirus software to safeguard.
- Remember to log off when you're done.



Stay Safe on Social Media

- Don't share provocative photos or intimate details online
- Be cautious when communicating with people you don't know in person, especially if the conversation starts to be about sex or physical details.
- Don't post or respond to anything online when you are emotionally charged up. Step away from your device.
- Don't get political. It's best to stay away from political and religious declarations which might seem abrasive and may offend others.
- Stay away from phishing Facebook webpage.

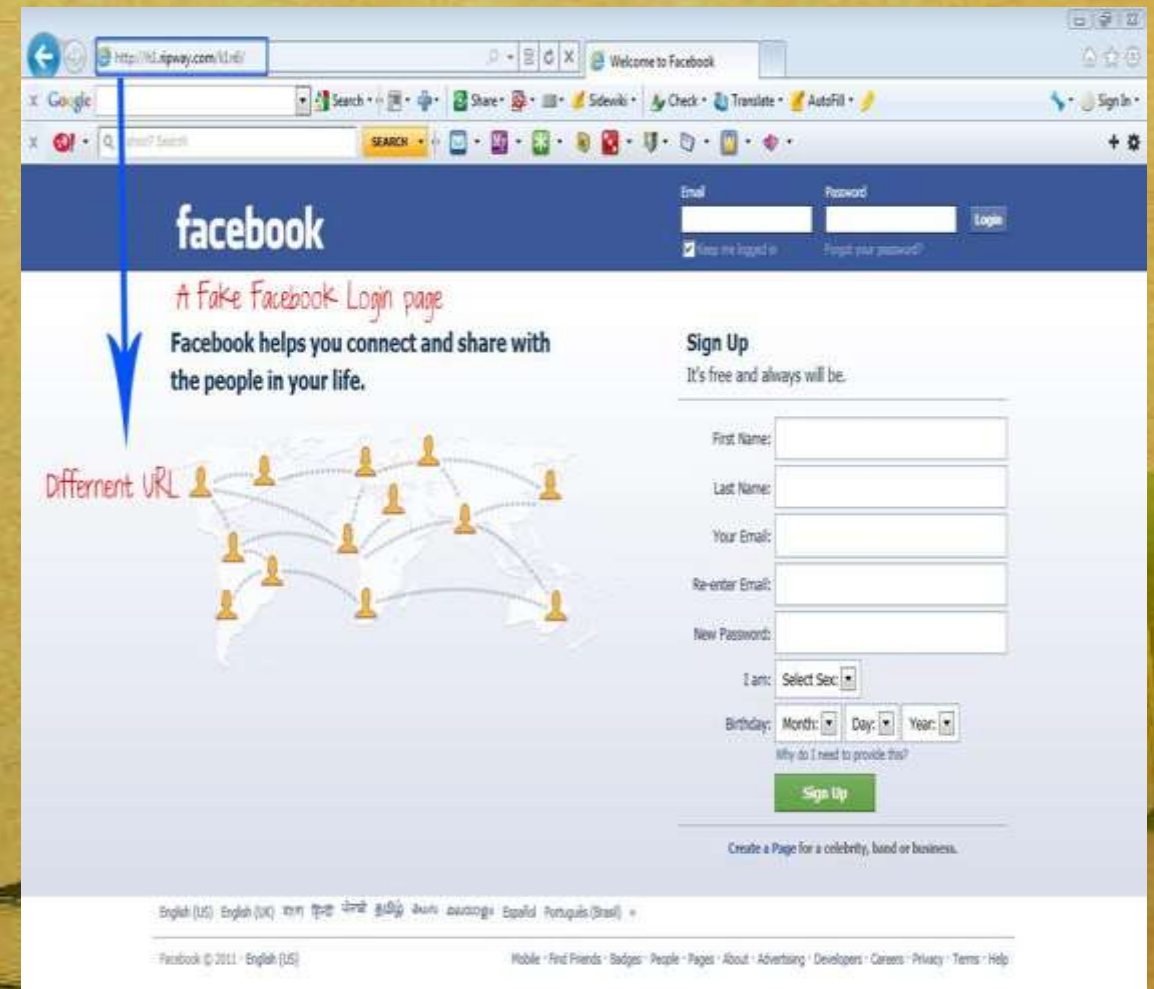
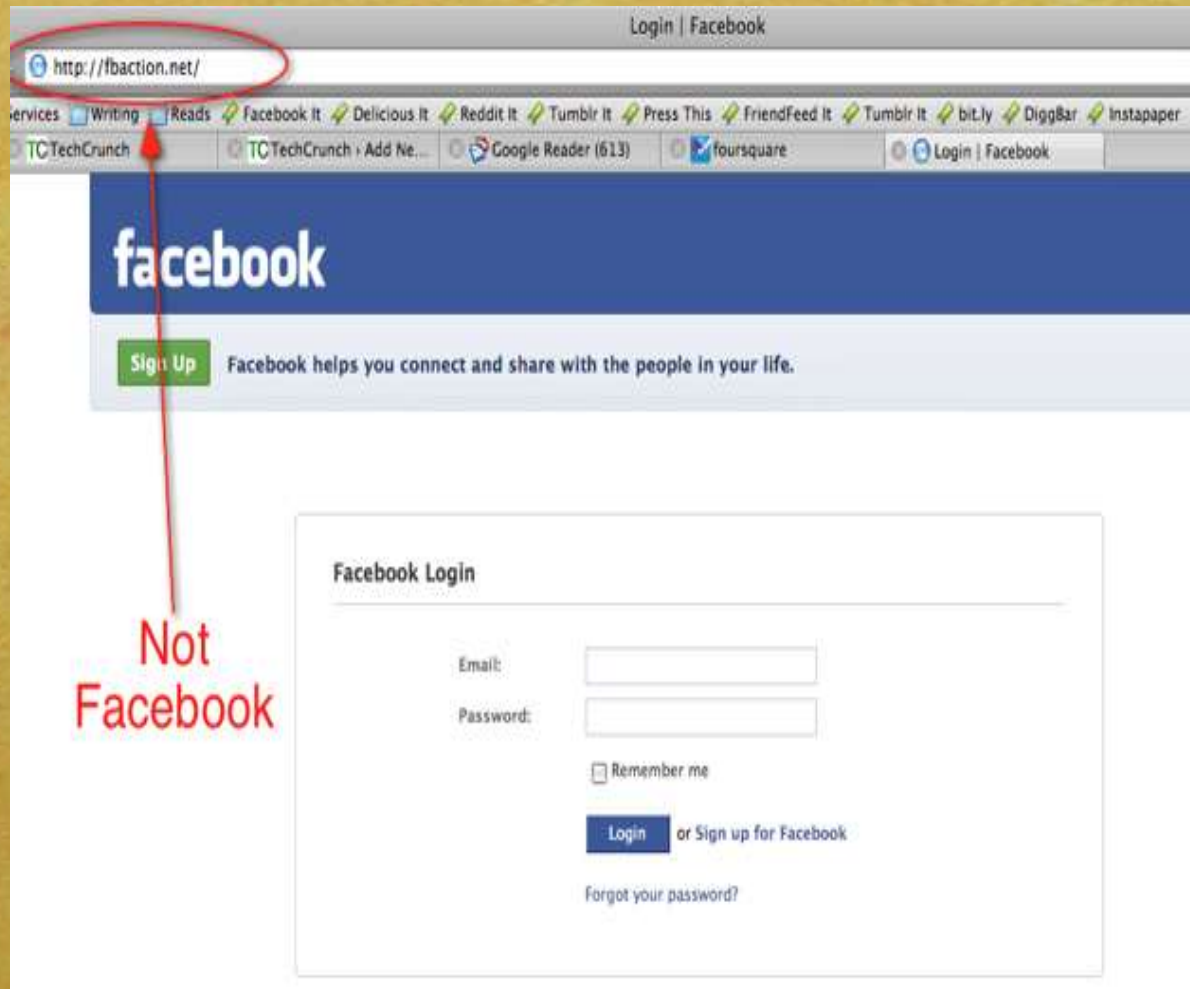


Stay Safe on Social Media

- Be careful while accessing your Social Media accounts in free Wi-Fi Zone.
- Hackers can intrude your system and steal your User ID / Password & also the banking credentials.
- Never access your online bank account or banking application in free Wi-Fi Zone.



Phishing Facebook Webpage



Point of Sale (POS)



Precautions to be taken at POS & Online purchase of goods

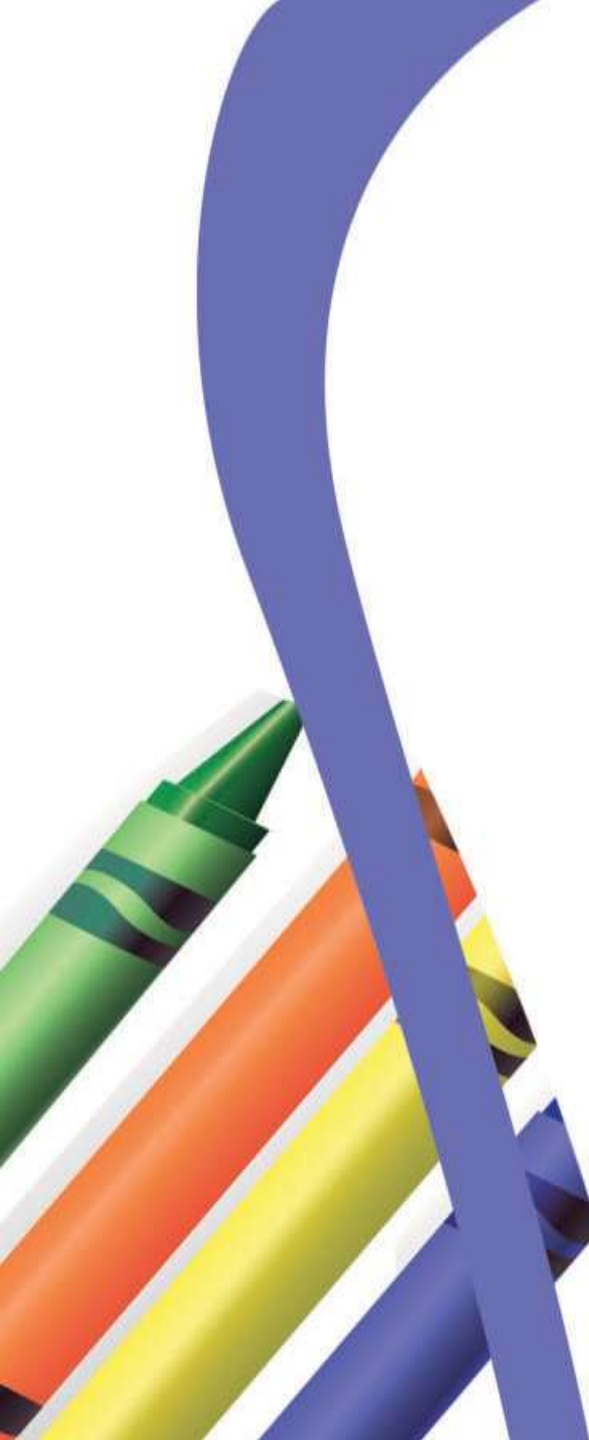
- At the time of purchase of goods or payment through card, use the Swiping Machine by yourself.
- Be careful at the time of entering of PIN Number.
- **Cover the keypad with your free hand so that nobody can see what you type in.**
- Look for the Skimmers.





Lottery Scam

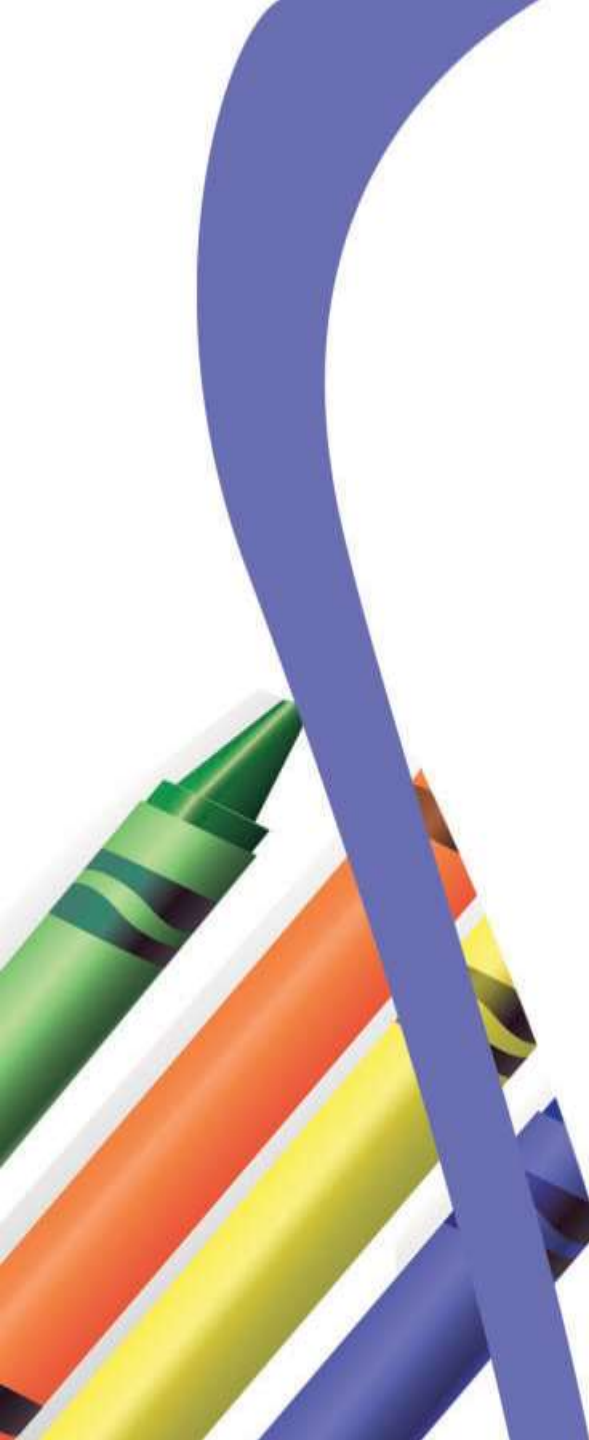


- 
- Lottery scam is otherwise known as Nigerian Fraud / Advance Fee Fraud / 419 Fraud.
 - If you will receive any phone call / messages / e-mails regarding winning of lottery, then don't attract into those fake offers.
 - Never deposit any advance money in the unknown bank accounts.
 - Never give your personal information or banking credentials over phone or e-mail.



INSURANCE FRAUD

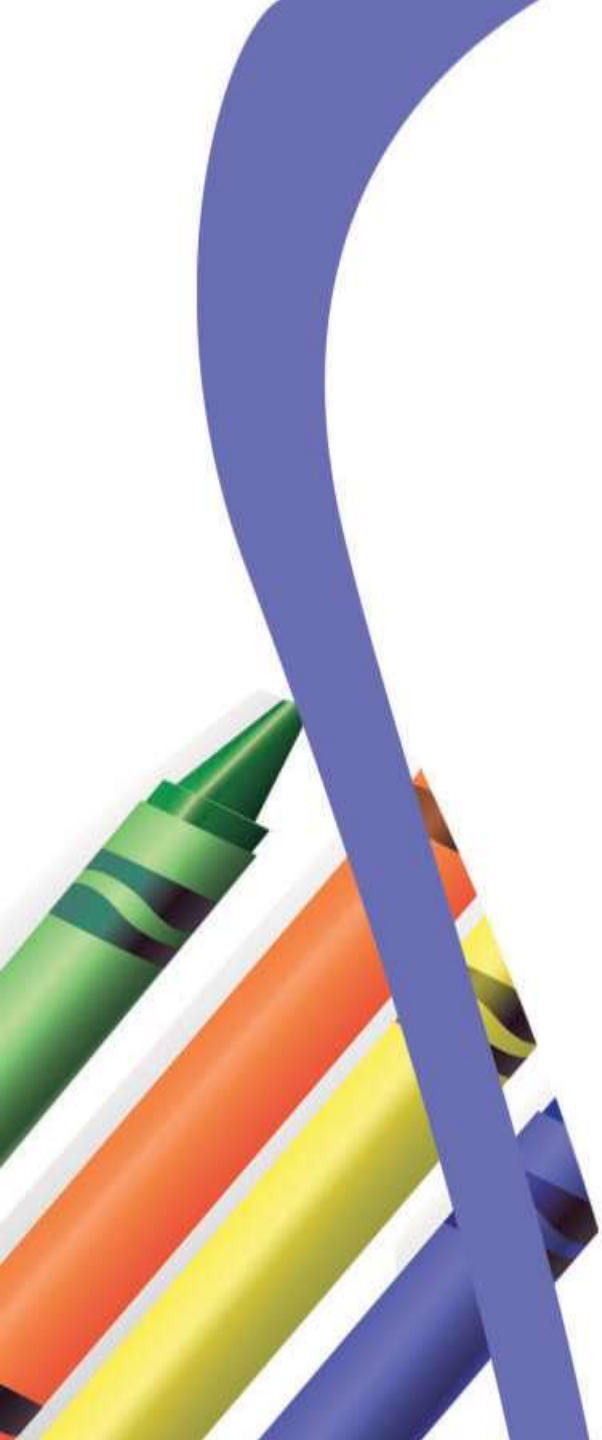


- 
- You will be told about “Your insurance policy is matured and you will get lakhs of rupees as matured sum of money”. If you will receive any such phone calls or come across any e-mails / messages, then don’t believe such phone calls or information.
 - It may be the call of FRAUDSTER.
 - Verify the authenticity of the information from your Insurance Company.
 - Don’t trust these phone calls of fraudsters and never deposit your hard earned money in the bank accounts of the fraudsters.



Job Fraud

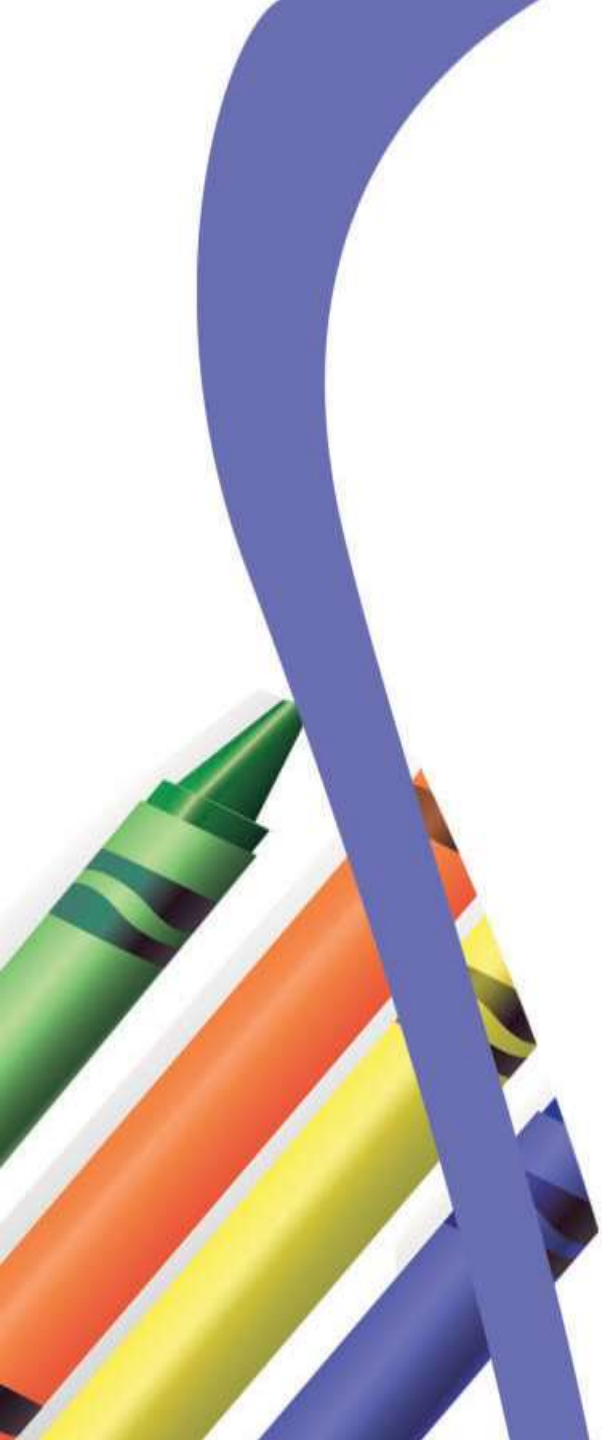


- 
- Advertisements are published in various popular newspapers and also **through online offering jobs inside the country & overseas.**
 - Fraudster will instruct you to send your personal information and to deposit money in advance in various unknown bank accounts or in Online Payment Gateway's Wallets towards processing fees.
 - **Verify authenticity of these advertisements and never deposit your hard earned money in the bank accounts of the fraudsters.**



Loan Scam



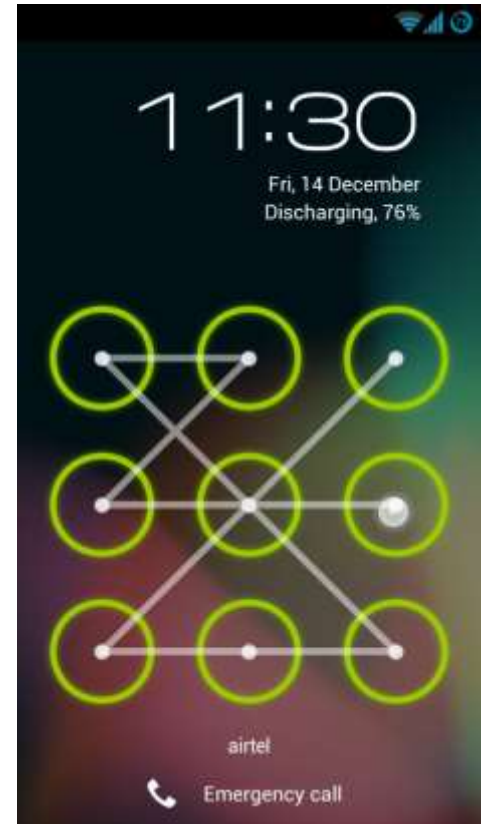
- 
- Advertisements are published in various Newspapers and also **through online offering instant loan to the tune of lakhs with less EMI .**
 - Fraudster will instruct you to send your personal information and to deposit money in advance in various unknown bank accounts towards processing fees.
 - **Keep away from these types of advertisements and never deposit your hard earned money in the bank accounts of the fraudsters.**

Mobile Phone Security





- Regularly update your Mobile Operating System & Software
- Auto-lock your phone
- Keep your mobile phone & various applications secure through strong password / screen lock / pattern lock / PIN lock
- Install Anti-Virus & Anti-Malware Software





- Back up phone data
- Avoid third-party apps. Read reviews, and if the app asks for access to too much personal data up front, don't download it.
- Use Public Wi-Fi carefully. Don't make banking transactions or transmit sensitive data while using it.
- If you bank or shop from your smartphone, log out of those sites once your transactions are complete.
- Turn off Wi-Fi and Bluetooth® when not in use



Precautions while using internet

- Be careful about fake website
- Operate your online banking account if the website domain name starts with https. It means all communications between your browser and the website are encrypted. https is used to protect highly confidential online transactions like online banking and online shopping order forms.
- Never access your online banking account at Cyber Cafes.
- **Don't operate your online banking account if the website domain name starts with http.**





Precautions while using internet



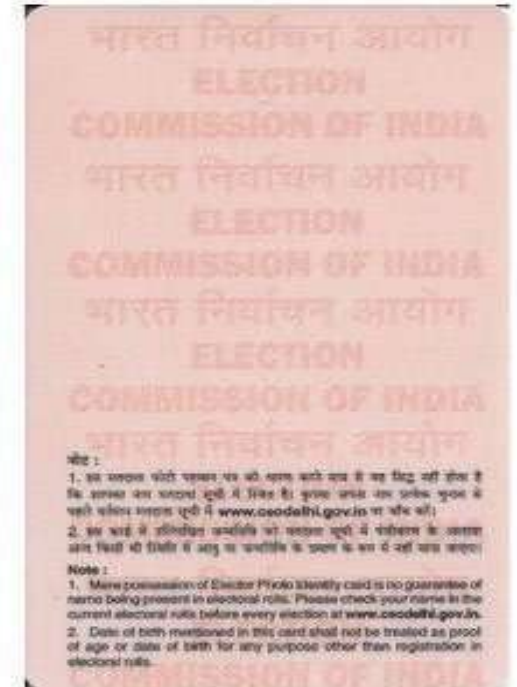
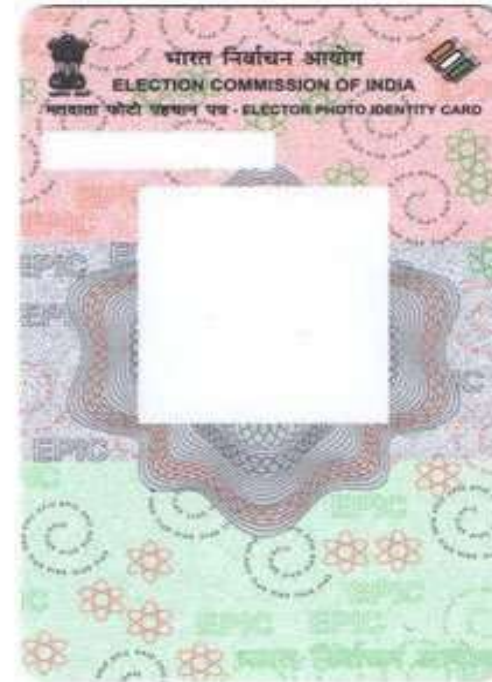
http




https



Precautions while submitting ID Proof documents

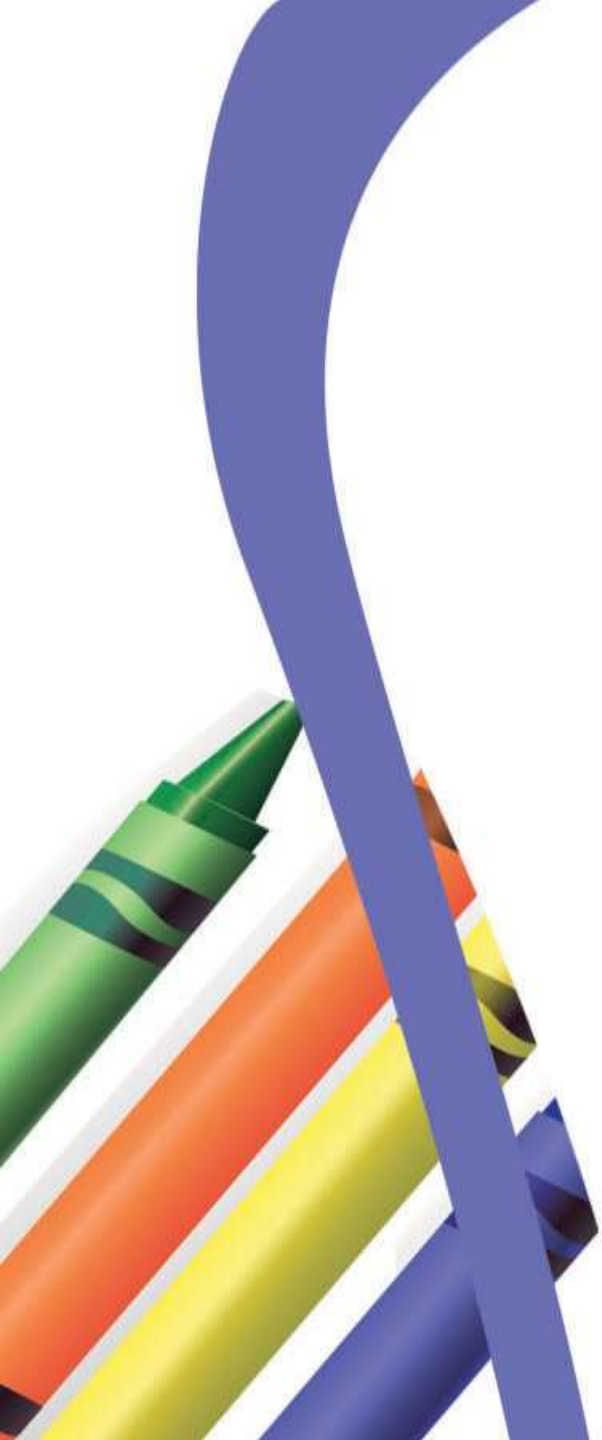


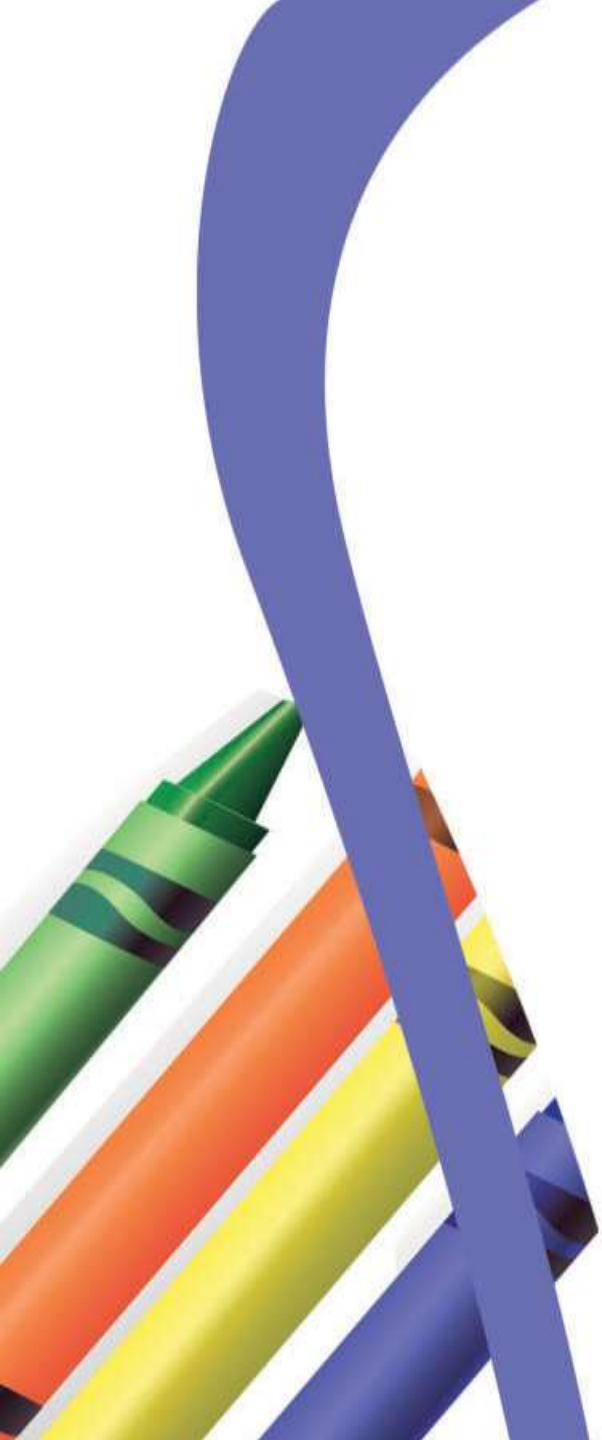
- 
- Generally at the time of procuring of SIM Card, opening of bank account, applying for loan, we are submitting photocopy of ID Proof documents like Aadhar Card, PAN Card, Voter ID Card, Passport, Driving License, Telephone Bill etc.,
 - To prevent misuse of your ID Proof documents, put your full signature with date and specific purpose.



Tower Installation Fraud



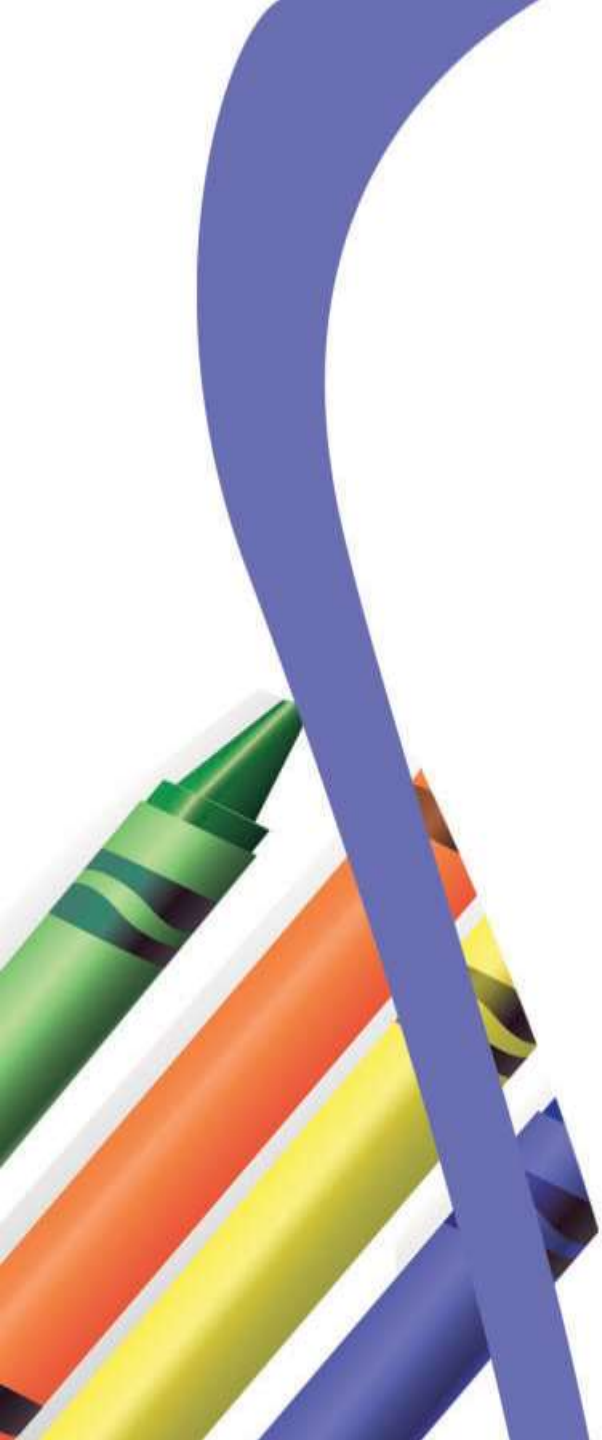
- 
- In various Newspapers, advertisements will be floated by the fraudsters towards installation of Telephone Tower and will instruct you to contact with them through mobile phone or e-mail.
 - When you will contact them, they will confirm your selection. They will also inform you about various processes involved towards winning of a huge amount of cash.

- 
- They will request the gullible public to deposit money in various unknown bank accounts towards Processing fees & clearance.
 - Don't trust in these phone calls of fraudsters and never deposit your hard earned money in the bank accounts of the fraudsters.



Face Recognition Scam



- 
- Recognize the face of Bollywood Heroes / Heroines and win handsome prizes.
 - These types of advertisements are telecast & published on Cable TV, Newspaper & Mobile Phone.
 - Fraudster will instruct you to deposit money in advance to claim the prize.
 - Keep away from such false advertisements and never deposit your hard earned money in the bank accounts of the fraudsters.

“Treat your password like your tooth brush. Don’t let anybody else use it, and get a new one every six months.”

-Clifford Stoll





Thanks

