# Goa Police

## Handbook on
## Recent common methods adopted by criminals to cheat

## Mode of cheating through phone calls

A call is made to the victim by the fraudster stating that they are from the bank head office and the debit card issued to the victim is blocked/expired. The fraudster then ask the victim for card details including CVV, OTP and PIN number for to renewal the card. The victim believing its genuine call from bank gives the card details. Once the card details are shared with the fraudster the fraudster after obtaining card details make online transactions or Point of Sale (POS) transactions.

**Actual Case**. A Victim was called over her phone by the fraudster and the fraudster introduced himself as the manager from the bank head office in Mumbai, in which the victim was having her bank account and Debit cum ATM card issued. The Fraudster further informed her that her card is blocked, and she needs to renew her card and get a fresh card issued else she will not be able to withdraw money from the bank. Believing that the call in genuine from the bank head office she gave her card details along with the CVV which is on the back of the card along with the PIN number of the card. Once the fraudster received the card details along with the CVV and PIN, he used the details on the ecommerce site and made online transaction, causing loss of money to the victim. When the money got deducted from her account she reported the matter to Police.

# Credit card fraud.

A call is made to the victim by the fraudster stating that they are from the credit card company informing card holder that huge reward points have accumulated and is due to lapse, and further ask the credit card details such as card number validity date, Card verification Value (CVV) and One Time Password (OTP) to transfer the reward points benefit. The victim believing its genuine call from credit card company gives the card details over the greed of getting huge reward points / gifts. Once the card details are shared with the fraudster the fraudster after obtaining card details make online transactions or Point of Sale (POS) transactions.

**Actual case**. A Victim was called over her phone by the fraudster and he introduced himself as the Manager of Credit Card issuing company. The Fraudster further informed the victim that his credit card has accumulated many reward points and he need to transfer the reward points as cash to the victim. Believing that the call in genuine from the credit card company, and out of greed to get the reward points as cash the victim gave his credit card details along with the CVV which is on the back of the card along with the OTP number of the card. Once the fraudster received the card details along with the CVV and OTP the details were used for online transaction, thereby causing loss of money to the victim. When the victim got his quarterly statement he realsied that his credit card is misused he reported the matter to Police.

## Cheating over story of finding treasure.

A call is made to the victim by the fraudster stating that he/she have found huge hidden treasure in form of gold/expensive stones and wants to sell it secretly. The fraudster lure the victim to sell it at very cheap rate, once deal is struck the fraudster then ask money for travel and other purpose and make victim deposit money into various bank accounts.

# Social media cheating.



The fraudster create fake profile showing them to be very handsome/beautiful looking pics with very rich business background and huge bank balance over popular social media site such as Facebook, Google+, marriage bureau sites, dating sites etc., They then develop friendship online with this victim. Once friendship is developed over constant touch online and the confidence and sympathy of the victim is won by the fraudster. Then fraudster make story that he/she is very rich and has lot of money in bank in foreign country. That they want to transfer money into victim accounts. And then on the pretext of tax, clearance charges makes the victim deposit money into various private bank accounts. Or make story that he/she has won a big business deal with huge profit margin and offer the victim to be partner into it, or ask the victim to help in getting start the business deal and ask for cash support. The fraudster offer huge profit margin for the contribution, and make the victim deposit the money into bank accounts.

**Actual Case:** - The fraudster created a very attractive profile on the social media site as a very rich doctor in the UK with a very handsome looking Profile Pic with very expensive cars and big castle in the background. The fraudster projected himself as a very wealthy man who is divorce. The fraudster then starts chatting with the victim, initially with casual chat, then then states showing interest in the victim to get married. The victim believing the profile that he is doctor by profession, who is very rich and handsome looking, in retune starts shows interest. The fraudster then make a story of coming to meet the victim and on the way at the Airport caught by the Airport authorities for not caring proper travel documents. The fraudster further states that the authorities has imposed fine on him and he has no sufficient money to pay the fine. He then ask the victim to send him money which he would return once he goes back to his native place after meeting the victim. The victim believing the story transfers/ deposit money into the bank account given by the fraudster.

# Cheating over the pretext of gift.



The fraudster create fake profile showing them to be very handsome/beautiful looking pics with very rich business background and huge bank balance over popular social media site such as Facebook, Google+, marriage bureau sites, dating sites etc., They then develop friendship online with this victim. Once friendship is developed over constant touch online and the confidence and sympathy of the victim is won by the fraudster make story of sending or coming to meet victim with expensive gifts including cash in foreign currency. Then the victim get a phone call informing that the caller is from customs department of some airport and the gift send/carried along by the fraudster is held back at the airport by customs department during delivery because it contains huge foreign currency, the fraudsters other member who pose as customs officer make the victim deposit huge amount to get the gift and the friend released by the customs department. If the victim pays the said amount the fraudster further make story that the gift is held back by Income Tax dept. or some other agency and make the victim deposit more money, till the victim realizes it a fraud.

The victim gets a friend request over a popular social media site from a person who is a friend of victims friend. As the person is her friends friend she accepts his friend request. After becoming friends they stated chatting for over a period of time. Then suddenly the fraudster make a story that he is sending her some gift as he cannot come and meet her. After 3 days the victim gets a phone call from a person who introduce himself as the Custom officer at Delhi Airport. He then informs the victim that there is a big parcel come in her name which contains huge foreign currency in UK Pounds, gold and Diamond jewellery and expensive phones and other gadgets. The person when poses as the Customs officer then send the victim a private bank account number in Delhi to deposit various taxes and fees amount to get the gift box released. Believing the story the victim over the greed of getting the gift box ends up paying huge amount into the bank account. Later when no gift box arrives after long date the victim then realized that she is cheated. She also released her mistake when she was pointed out that government taxes and fees are never paid into any private persons bank account.

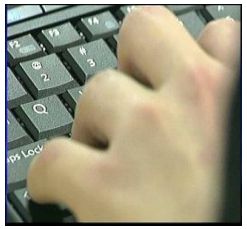
# Cheating through email/ SMS

The fraudster send SMS, Chat Messages or emails to victim informing that they have won big lottery prize for very huge amount, and further inform that to claim the prize they need to pay the taxes, fees and various charges in advance. The fraudster then make the victims deposit money into various bank accounts as tax process fees etc. The victim over the lure of getting huge lottery prize amount end up paying money into various bank account believing that they are taxes, process fees or charges which are required to be paid in advance.

# Marriage site cheating

The fraudster make fake profile showing them to be very handsome/beautiful looking pics, young age with very rich business background and huge bank balance. The fraudster then Shows interest in victim to get married. The fraudster then stats keeping regular contact with victim online or over phone. After some time once the friendship and confidence is developed the fraudster make story of money being blocked in bank for technical reason, and further shows to have got big business project with very huge profit margin. The fraudster convince the victim to help temporary till bank account matter is resolved and make them transfer amount into various banks. Or make story of meeting with accident and in need of urgent money and make the victim transfer money into various bank account. The victim as developed immortal attachment transfer the money believing the story and end up cheated.

# Online job cheating.



The fraudster obtain data from genuine job portal sites. The fraudster creates a email address which looks very close to any big business/ Industry. The fraudster then contact the victims over emails from the typo type email address created by him with some scanned / forged letter heads. The victim is then send mail stating that they are shortlisted for high post job for very attractive salary mostly in foreign countries. The victim believing it to be genuine email from a genuine company and as the victim had registered online believes the email received. The fraudster then make the victim go through short online interview by making them pay charges. After the interview the fraudster says that the victim is selected and further making them pay for visa clearance and for other purpose. Believing the fraudsters story and being happy of getting good job with high pay the victim end up paying huge amount and gets cheated for job for which the victim was never selected.

The Victim had uploaded her resume on a genuine job portal for seeking job abroad in pharmaceutical company for higher pay. After some days the victim gets a mail from a email address linked to a very big pharmaceutical industry in the US, informing her that her resume is shortlisted, and she was asked to send her scanned documents along with her passport copy. After some days she again get a mail informing her that her online interview is fixed on a date and time over phone. On the said date she attends the interview, the interviewer who speaks foreign accent ask her few technical questions and then tells her that she is selected for the job. He then gives the reference of a person who is from the US consulate and who would be contacting her for her further travel and visa documentation. After few days she gets a mail which appears to be sent from the US consulate asking her to deposit money for travel charges, visa process charges and other charges. The person makes the victim believe that all the money which she would be depositing would be refunded back to her once she join the job. Believing the story the victims pays money into the private bank account number given. Once the amount is deposited the fraudster further keeps on asking more money over the pretext over some other charges and fees. The victim in total paid Rs. 13 Lakhs. When the fraudster further started asking for more money the victim shares the incident with her family members and then she realized that its a fraud.

# Website fraud.

The fraudster creates sites with very attractive domain name or with domain name very close to popular ecommerce sites with similar looking home page. The site then offers things at very cheap rate. The victim is then made to make the payment first for the cheap product delivery. Once the payment is made the delivery is never made and the victim gets cheated. Or the fraudster offer expensive product at very cheap rate on genuine sites such as OLX, quikr or E-bay. Then the victim is made to send the payment in advance for the delivery of the product. Once the money is send the product is never delivered and the victim is cheated.

**Actual Case**:- The victim saw a add on a site for sale of New Ipad for Rs. 8,000/- as an offer sale. The victim then contacted the phone number given on the site for further details. The fraudster at the other end asked the victim to deposit into a private bank account amount of Rs. 8000/- for the delivery of the Ipad. Once the amount was deposited the fraudster further asked money saying that he would get an additional New Iphone 6 for Rs.10000/-. Believing the story the victim further deposit Rs.10,000/-. Once Rs. 10,000 was received by the fraudster, he asked the victim to deposit another Rs. 20,000/- as tax and duty as it's direct imported gadgets. The victim deposits Rs.20,000/. Finally nor the Ipad or the Iphone is delivered tot the victim and the victims ended up losing huge amount which is much more then the actual price at which Ipad is available at authorized stores.

# Wealthy heirs story

The fraudster sends a email or SMS to the victim making a story that his Grandparents have left back huge wealth in the form of bank balance and property, in a war effected country. The fraudster further makes the victim believe that he need to transfer the wealth and wants to sell the property and the amount derived from the sale of property to the victims name as he / she is living in a peaceful country. The fraudster offer huge amount of share from the to be transferred amount. Believing the story and out of greed the victim agrees to get the amount transferred in his /her name and bank account. The victim is also made to give his/her document proof and bank details. After some time the fraudster make a story that the money is transferred from his country but held back by the International Monitory fund (IMF) as it's a very very huge amount, and in order to release the amount certain amount is required to be paid. The fraudster then make the victim deposit amount into a bank account for the release of money held back by IMF. Then he makes story of amount released by IMF but held back by the UN Anti Terrorism Squared. The fraudster then again make the victim deposit money for the release of amount from UN. Then he says that the European Union (EU) has held back the money as no taxes are paid, and make the victim deposit amount as taxes. By the time the victim realizes it's a fraud the fraudster end up cheating the victim for a huge amount.

## Income tax return fraud and Insurance policy maturity amount transfer fraud

The fraudster obtain the PAN card and other details of the victim from social media sites. The fraudster then calls up the victim and inform that some amount of income tax deduced by mistake is required to be refunded back to him. The fraudster then ask for the bank details for transferring the amount. The victim out of greed for money and believing the story gives his bank details. Once details are sent the fraudster ask the victim to pay the taxes over the amount he is going to revive to be paid in advance. Believing the story the victim pays the amount as advance tax into a private bank account, and ends up cheated and loosing money

The fraudster makes a call to the victim informing that an insurance policy has matured and he is the nominee to that insurance policy. The fraudster then ask for the bank details for transferring the amount. The victim out of greed for money and believing the story gives his bank details. Once details are sent, the fraudster ask the victim to pay the taxes over the amount he is going to revive to be paid in advance. Believing the story the victim pays the amount as advance tax into a private bank account, and ends up cheated and loosing money

## Cheating over offer of cheap loan with no surety

The fraudster send email or SMS or put up advertisement on new paper offering loan /finance at a very cheap rate of interest with no surety. The fraudster then gives a contact number of email address to contact them back. Once the victim contact back, the fraudster gives them very attractive loan /finance for huge amount, over very cheap rate of interest with no surety. Once the confidence is won by the fraudster, he then ask the victim to deposit certain amount of money in a particular bank as processing charges, then additional amount for agreement drafting charges and stamp paper charges, the fraudster keeps on demanding money over various pretext till the victim realizes that it's a fraud and he/ she is being cheated.

The fraudster puts up an advertisement in a local daily news paper offering finance /loan to prospective businessman for 2% rate of interest with no surety. The victim called back the fraudster on the given number, and expressed his interest in finance. The victim was asked by the fraudster to deposit money in a particular bank account as processing charges. Once the money was deposited the fraudster kept on asking for more money, and when more and more money was demanded the victim realised that she was cheated.

# Caution

If you come across any of these situation, ***please be cautious it is a fraudulent act***, please do not share any of your bank details, or deposit any money in any bank account.

Immediately report the matter to Goa Police on following contact details.

Police Control Room Phone No. **100**
Goa Police email ID:- **goapol@bsnl.in**

Cyber Crime Police Station Phone **0832-2443201**
Cyber Crime PS email ID picyber@goapolice.gov.in

**Or Contact your nearest police station.**

***A initiative of Cyber Crime Police Station, Ribandar, Goa.***