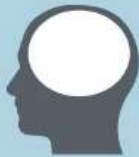


# CYBER SECURITY

## LATEST FRAUD METHODS - 1 OF 3

Abstract from meeting with Raipur Police - Cyber Crime Team



### VIDEO CALL

Do not pick video call from an unknown number. Screenshot/video can be taken with your face and objectable video from the other side and later blackmail.

### SEPARATE HANDSET

Do not give smartphones to children with google pay/wallets or SIM where you get banking OTPs. Gaming app have very easy way to take money in few clicks.



### CALL FORWARDING



A fraudster may ask you to dial \*401/403\* <10 digit number>. An indirect way for forwarding your calls. CALLs will be forwarded to them including OTP over call.

### WHATSAPP DP FRAUD

Be alert if you get any money requests from an unknown number. They may put DP of your boss, colleagues, friend or family.



### LOAN APPLICATION

Do not fill out any loan or any application on an untrusted site. Your vital KYC info may be in the wrong hands.

### CLICKING LINKS



Be vigilant for clicking any link (over Whatsapp, SMS, email, etc). You may be downloading some app or passing personal info.

# CYBER SECURITY

## LATEST FRAUD METHODS - 2 OF 3

Abstract from meeting with Raipur Police - Cyber Crime Team



### QR CODE

Remember QR code scanning is for Payment and NOT for receiving money. Fraudsters may promise you to send money if you scan the QR code sent by them. A trap.

### OLX FRAUD

Asking you to pay in advance for selling used vehicles/appliances/furniture. They look genuine (e.g. posing as ARMY officers on transfer)



### KBC FRAUD



Lottery offer, collection of money or personal information

### GOOGLE SEARCH FRAUD

Usually, Google search will display 2,3 ads on top of their search output. Be careful on clicking and getting any customer service number. You may call a fraudster.



### OTP

Old but still the most used technique. NEVER EVER share OTP with an unknown person (they may pose as bank/police / govt agency etc)

### ACCESSING PHONE



Alert if an application gets downloaded. Say no to remote viewing apps (anydesk etc). If someone can read your phone, you are gone.

# CYBER SECURITY

## SAFEGUARDING YOURSELF

Abstract from meeting with Raipur  
Police - Cyber Crime Team



### SPEND MIN/NO TIME

Almost all fraud has a history that person has spent a good amount of time with the fraudster. The more you talk to an unknown person, the more chances of the trap. If you get a good offer, cut the call, verify the info and try from your side if find it genuine

### CALL INCOMING / OUTGOING

Fraudsters will try to reach you, not vice versa. One needs to be on alert while getting calls from unknown asking for information (e.g . kyc update, credit limit increase, card block etc)



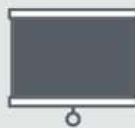
### 2-STEP VERIFICATION



Whatsapp 2-step verification ensures the need of a PIN when registering a phone no with whatsapp again. Gmail sends notifications in case of login in new device.

### RS 10/- FRAUD

You will be asked to pay Rs 10 or some minor amount for registration or account opening or KYC. You are exactly doing what fraudster want you to do.



### FRAUDSTER'S SKILL

Fraudsters are always a step ahead of the system. They work like professionals. There are big training institutes for training them. They find new and good techniques. One needs to be vigilant always .



### PREVENTION IS KEY



Police may catch the fraudster, conditional on Police bandwidth and prioritization. Remember, the first fraudster's bank account where your money land, is most likely bogus making the police job difficult. Prevention is the key.