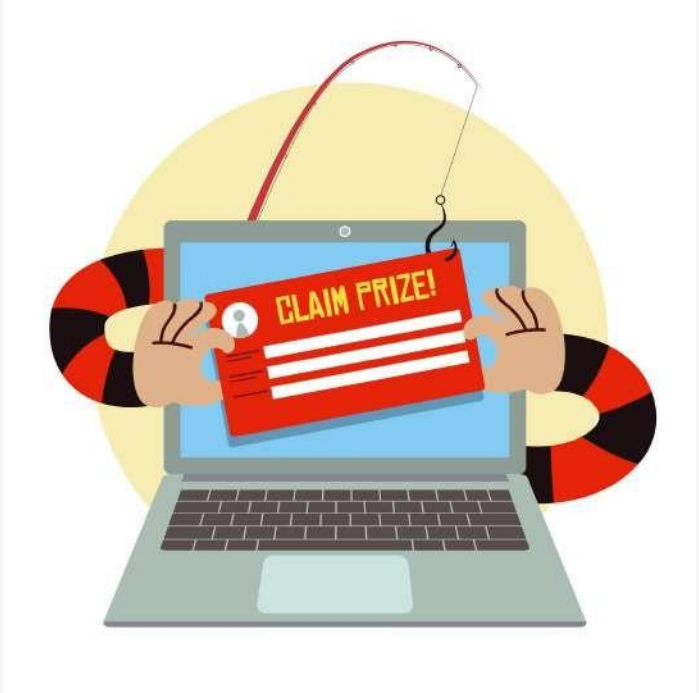
Protect Yourself in the Digital World

Kerala Police

Lottery Fraud / Fake Prize Frauds

The fraud in which, victims receive phone calls, emails, SMS's, WhatsApp messages, or letters etc. telling them that they have won a lottery or an expensive gift. Victims are subsequently requested to deposit money in a bank account as processing fee or tax. Once the money is sent, victims never receive the promised prize and get cheated.



Modus Operandi

1. Scammer sends lottery emails/SMS to victims, claiming they've won lakhs in a lottery.

2. Victim excitedly responds via email, providing personal details as instructed by the scammer.

3. Scammer sends a scanned copy of a forged cheque/certificate in the victim's name.

4. Victim, believing the scam, deposits money into a fake bank account provided by the scammer as a "registration fee."

5. Victim may end up depositing large sums, sometimes exceeding lakhs, into multiple fraudulent accounts.

6. Ultimately, the victim realizes they've been scammed, losing significant amounts of money to the fraudster.

Never transfer money to anyone in the name of a lottery or gifts.

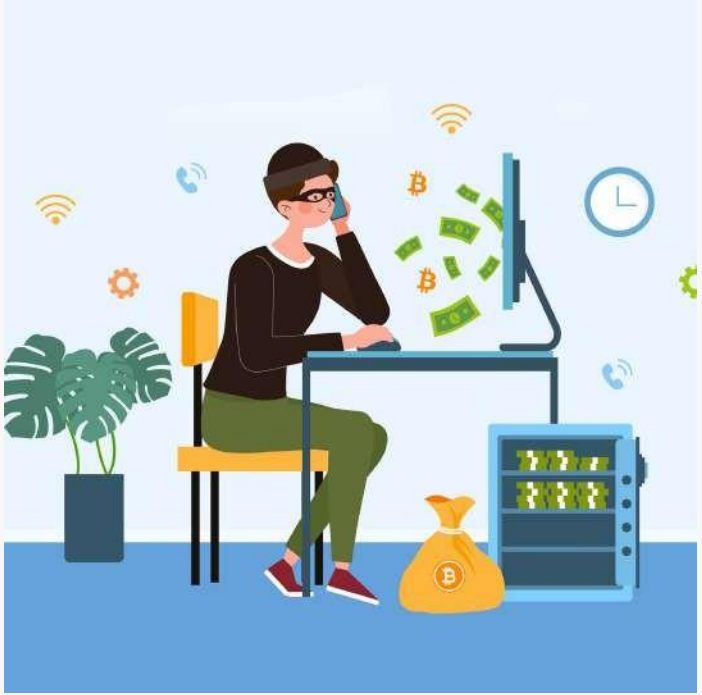
Never respond to unsolicited offers received through emails, messages, phone calls, and other social media.

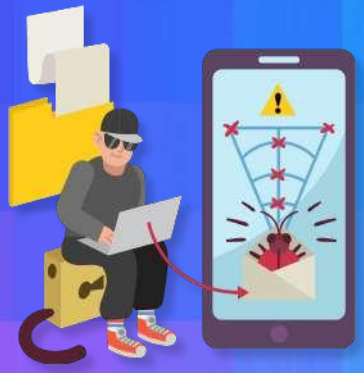
Legitimate lotteries or giveaways do not require payment to receive winnings.

NO LEGITIMATE LOTTERY WILL REQUIRE YOU TO PAY ADVANCE MONEY.

Investment/Trading Fraud

Cybercriminals creates fake investment opportunities advertised through spam emails, online advertisements, or social media platforms. These schemes promise high returns with minimal risk but are designed to defraud investors by either stealing their funds outright or using them to perpetuate other fraudulent activities.





Modus Operandi

1. The victims receive advertisements about free trading tips classes on social media platforms like Facebook, WhatsApp etc.
2. When they click on the advertisement, they will be redirected to an unknown WhatsApp / telegram group.
3. Fraudsters communicate with the victims via these groups and persuade them to invest by offering them free trading tips to buy and sell stocks.
4. After a few days, the victims are asked to install trading applications provided by the fraudsters for further guidance in trading stocks and earning huge profits.
5. Fake profits are displayed in the digital wallet.
6. When victims try to withdraw their ‘profit’ from the digital wallet, they are told that this is possible only if they reach around ₹50 lakh or above in profits.
7. Trusting this as company policy, the victims continuously invest, as per the instructions of the fraudsters
8. When try to withdraw the invested money, fraudster ask victim to pay tax or any other fee.

Investors and traders should exercise caution and skepticism.

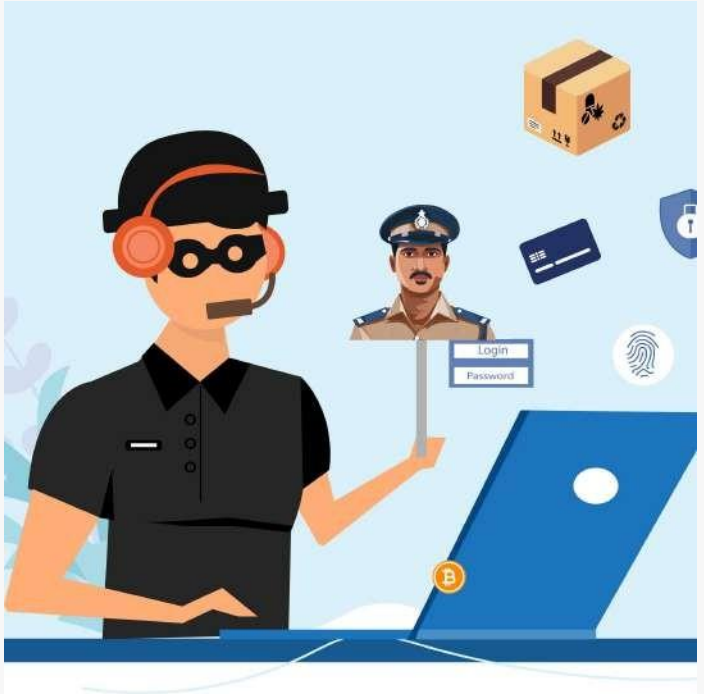
Conduct thorough due diligence before investing.

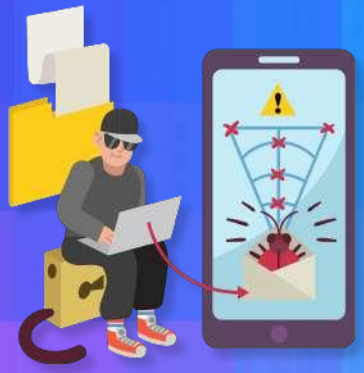
Be wary of investment opportunities that seem too good to be true.

DO NOT INVEST IN ONLINE TRADING PLATFORMS THAT PROMISE HIGH RETURNS.

Threats of Illegal Goods Delivery
(FedEX scam)

Cyber fraud related to threats involving the delivery of goods misrepresented as narcotics or illegal goods, typically involves scammers posing as law enforcement officers, customs officials, or representatives of courier companies. These scammers use various tactics to intimidate victims into believing that they are involved in criminal activity or are at risk of legal consequences unless they comply with their demands.





Modus Operandi

1. Victim receives unsolicited communication from purported law enforcement or courier company.
2. Scammer claims a package with illegal items intercepted, implicating the victim.
3. Victims threatened with legal consequences unless they comply with payment demands.
4. Victim pressured to pay a fine or provide personal/financial details.
5. Intimidation tactics used, including aggressive language and deadlines.
6. The victim will be intimidated telling that they are under virtual Arrest.
7. Scammers exploit fear to prevent victims from seeking help.
8. Payment demanded via untraceable methods like wire transfers or cryptocurrency.
9. Scammer may persist with threats even after initial payment

Report suspicious communications to relevant authorities.

HELPFUL TIPS

Verify with legitimate authorities using official contact information.

Stay updated on common scams and fraud tactics to prevent future victimization.

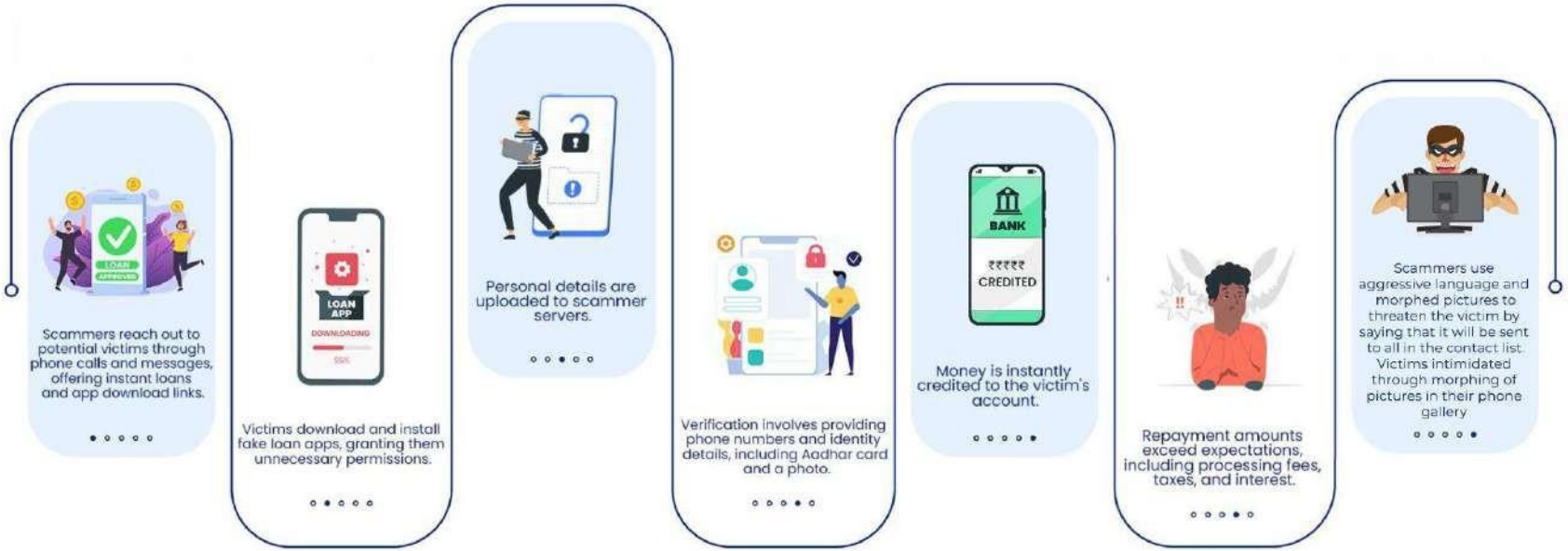
Refuse payment or sharing personal/financial details until legitimacy confirmed.

NO ENFORCEMENT AGENCY WILL ASK YOU TO TRANSFER FUNDS. THEY HAVE POWER TO FREEZE SUSPICIOUS ACCOUNTS.

Fraudulent Loan Apps Exploiting Low-Income Individuals

Fraudulent loan apps promise quick loans with minimal documentation, often targeting low-income individuals in urgent need of funds. These apps typically require personal and financial information as part of the application process. Many of these apps charge exorbitant interest rates or hidden fees, trapping borrowers in debt cycles. Scammers resort to various tactics to threaten the borrowers when they fail to repay, including defamation and threat.

Modus Operandi



Avoid availing loans through Loan Apps

Read app reviews and verify permissions accessed

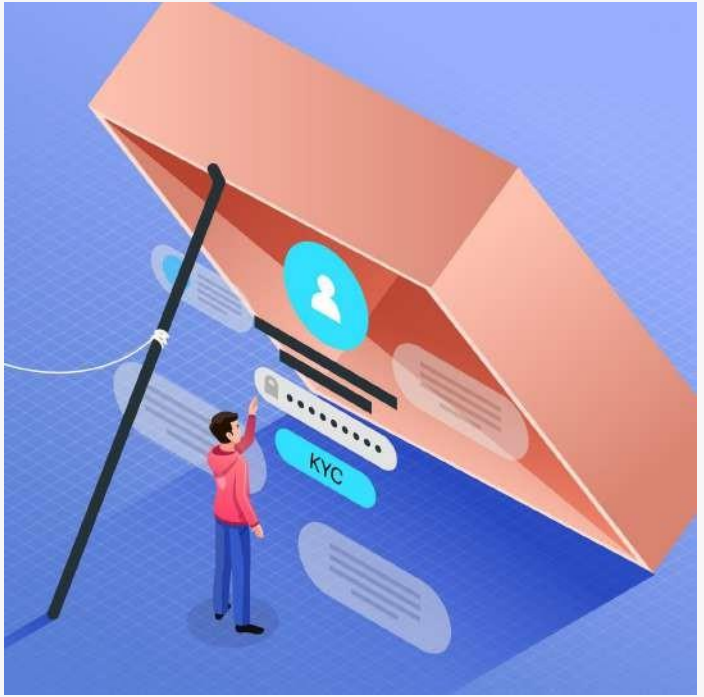
Never use 3rd Party Applications

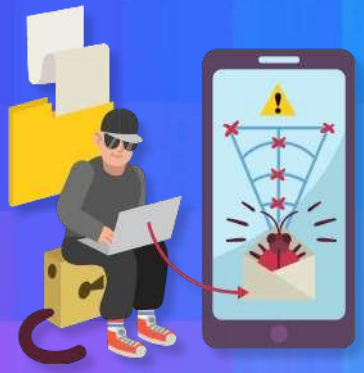
Avoid APK files send through links and don't share OTP/PIN

KEEP AWAY FROM LOAN APPS. RELY ON YOUR BANKS.

Credit/Debit Card, KYC Expiry/Renewal Frauds

This type of fraud involves manipulating victims into believing they are complying with legitimate requests from their bank such as expiry/renewal of KYC, credit/debit cards etc., while in reality, they are being deceived into installing malicious software, providing sensitive information, and ultimately falling victim to unauthorized fund transfers. The fraud involves a type of phishing scam combined with social engineering tactics and unauthorized access to personal devices.





Modus Operandi

1. The fraudster pretends to be a bank officer , makes calls or sends an SMS or a link to the victim to update KYC for uninterrupted service.
2. The fraudster sends a link to the victim and tells the victim to click the link and install the application. This application may be like Team Viewer, quick support, Any-Desk, and the fraudster can see the activities in our mobile phone.
3. The fraudster tells the victim to make a transaction of a very small amount to update KYC and the victim does this transaction.
4. The fraudster gets bank/ wallet credentials from the victim.
5. The fraudster transfers the money from the victim’s bank account to his/her wallet/bank account.

Verify all bank communications directly.

Avoid clicking links from unknown sources.

HELPFUL TIPS

Don't install apps recommended by strangers.

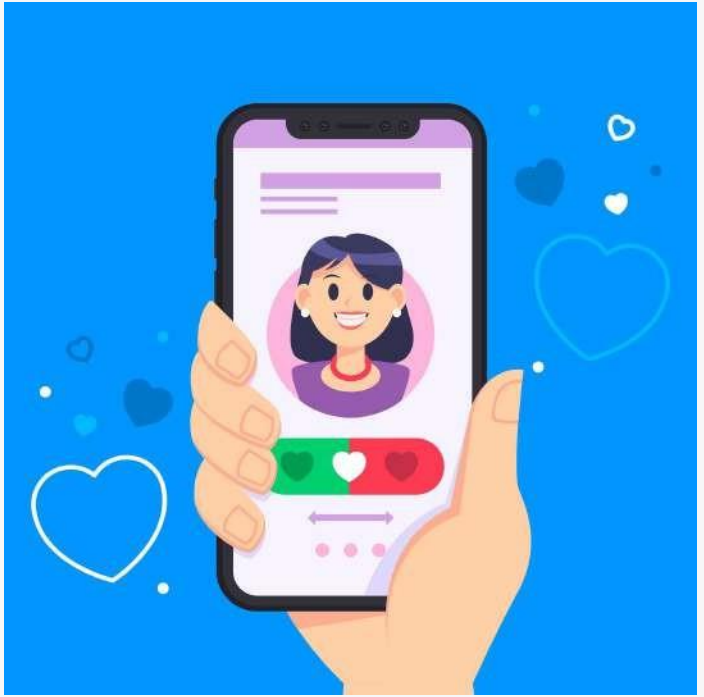
Monitor account transactions regularly.

LEGITIMATE SERVICE PROVIDERS DO NOT ASK FOR PERSONAL CREDENTIALS OR ASK TO INSTALL ANY APPLICATIONS.

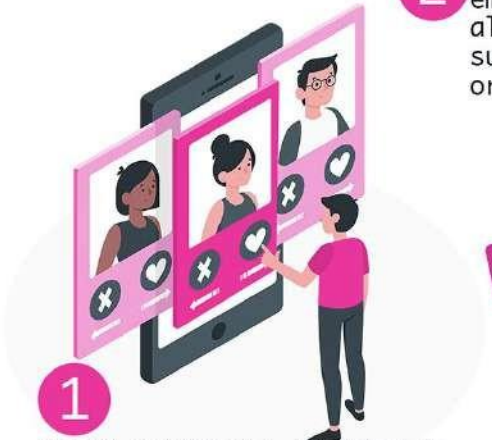
SEXTORTION

Sextortion is extorting money or sexual favours from people by threatening to reveal evidence of their sexual activity. The fraudsters try to lure the users into sharing intimate content in different ways such as

- ❏ Posting messages for video/audio chat
- ❏ Using fake accounts/profiles
- ❏ Creating pages/Ad. campaigns



Modus Operandi



1 Cyber-criminals pretend to be young women on dating apps, cat-fishing people and gathering their personal information. Once targets are identified, they lure them with photos and invite them for real-time video chats.

2 They express strong emotions too fast and almost straight away suggest to get nude or sexual in a video call.

3 The offender will then record the entire activities.

4 Threatens the victim that those videos will be published if they don't pay money.

5 Blackmailing often continues even after victims have paid.

Avoid video calls from unknown and Don’t get too much private with strangers.

Do not give them any money or send any more pictures of yourself. It will only result in more demands for payment.

HELPFUL TIPS

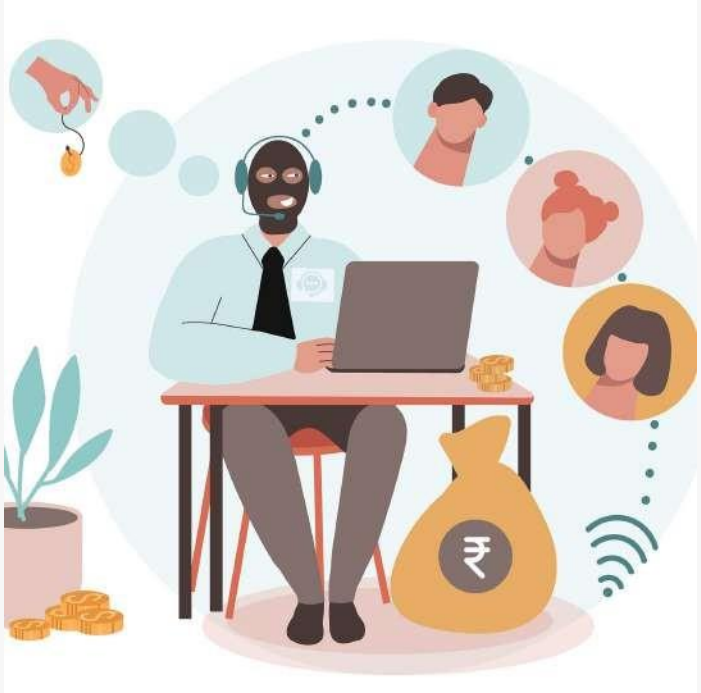
Report to the relevant social media platform.

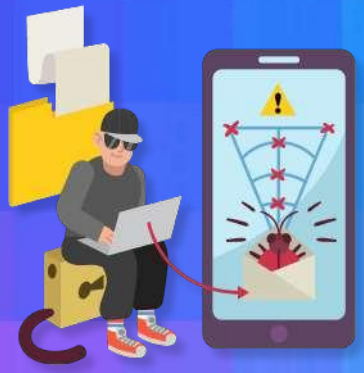
Stop all contact with the blackmailer

DO NOT ATTEND VIDEO CALLS FROM UNKNOWN NUMBERS.

Fraud Involving Fake Customer Support

Fraudsters exploit the reliance on customer service by setting up fake support teams to deceive customers. They distribute fake contact numbers through online platforms like blogs and manipulate contact details on platforms such as Google Maps. Victims unknowingly contact these fake teams, follow their instructions and lose money.





Modus Operandi

1. Customer service is a very important part of every business. Whenever customers face any problem, the first thought is to contact customer care and tendency is to find customer care contact through online search engines like Google.
2. Fraudsters set up fake customer support teams to cheat customers.
3. Fraudsters post their numbers on the internet as customer care numbers, either by commenting on popular blogs or by publishing blogs with their numbers.
4. They also replace the original number of the banks, shops or any other establishment by editing the contact details on Google Maps.
5. Customers unknowingly contact these fake support teams, believing them to be legitimate, and become victims.

Customers should verify contact details from official sources

Exercise caution when sharing personal information online.

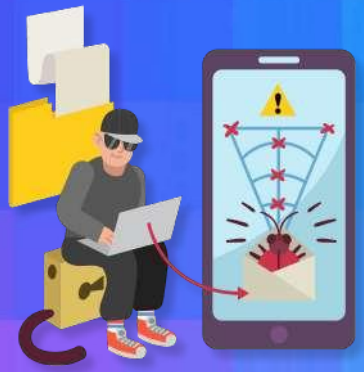
Always search for customer care number from the official website of the entity

Toll free/customer care numbers of banks will be given on the back/flip side of debit/credit card, Bank passbooks etc.

SEEK CUSTOMER SUPPORT ONLY FROM AUTHORIZED WEBSITES OF THE SERVICE PROVIDER. DO NOT SEARCH FOR CUSTOMER SERVICE ON GOOGLE.

Romance Scam: Deceptive Gifts

Romance scammers, often posing as individuals from foreign countries, target victims on dating platforms and social media. They build trust with victims, promising to send valuable gifts via international parcels. Fake Customs officers then demand customs fees, prompting victims to send money to a specified account. After payment, victims never receive the promised gifts, and the scammer disappears



Modus Operandi

1. Romance scammers, often claiming to be from Australia, the UK, or the US, use fake profiles on dating platforms or reach out via social media like Instagram, Facebook, or Google Hangouts. They build trust by fostering a relationship, often engaging in frequent communication.
2. After weeks or months, they claim to send valuable gifts like designer items, laptops, and smartphones via international parcel with a tracking number.
3. Victims receive messages from fake Customs officers, demanding customs fees to release the package, with a specified bank account or money transfer service for payment.
4. Once the money is sent, the package never arrives, and the scammer vanishes, cutting off all contact.

Be cautious when interacting with individuals online, especially on dating platforms and social media.

HELPFUL TIPS

Verify the identity of individuals you communicate with through online searches or additional photos.

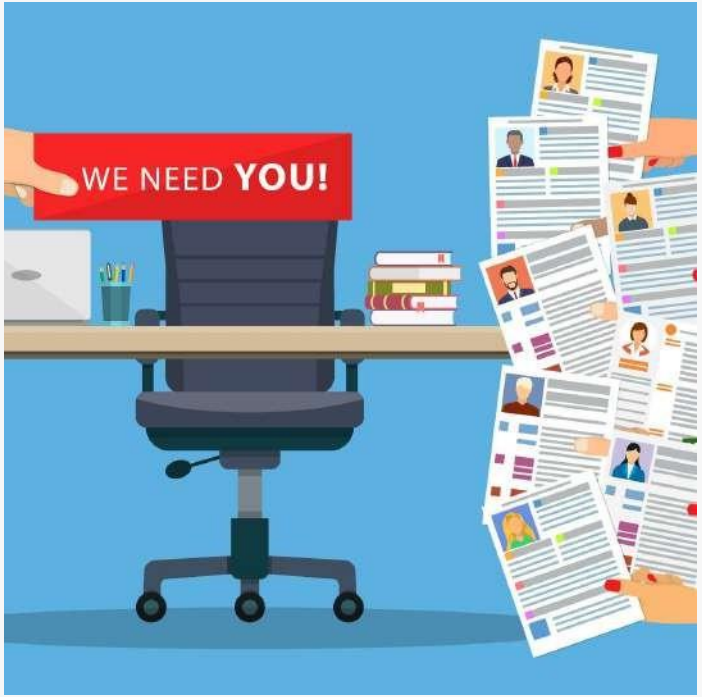
Never send money or provide financial information to someone you've only met online.

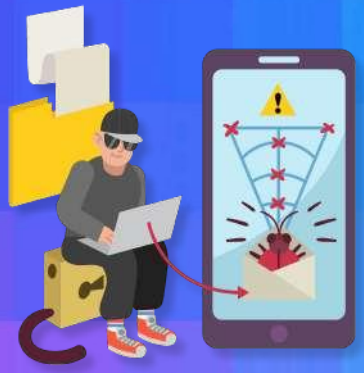
Familiarize yourself with legitimate customs procedures and be skeptical of unexpected customs fees.

ALL GIFTS THAT REQUIRE YOU TO MAKE ADVANCE PAYMENTS ARE FRAUDULENT.

Scams Targeting Job Seekers through Fake Job Offers

Cyber criminals advertise fake job offers using various online platforms like social media, fake websites etc. Victim, in search of a job, goes through these fake job offers and contacts the cybercriminal. Victim follows the guidelines of the fraudster for getting a job and falls prey to the cyber-crime.





Modus Operandi

1. Fraudster pretends to be an employer or recruiter, enticing job seekers with promising opportunities that involve upfront payments, like visa fees, travel expenses, or credit checks.
2. Scammers easily target a wide audience by posing as job consultants on popular job portals like Monster, Naukri, Times Jobs, and Shine etc.
3. Scammers send mass emails requesting security deposits or interview fees to schedule interviews.
4. Scammers conduct fake online interviews before sending bogus appointment letters.
5. Fraudsters send call letters and collect fee towards uniform and other processes.
6. After the money is paid, the scammer vanishes, leaving the job seeker without a job or a refund.

Do your research. Contact the prospective employer directly to verify whether the listed position is available.

It's a fake job call if you are asked to disclose your date of birth, social security number or any other personal details.

HELPFUL TIPS

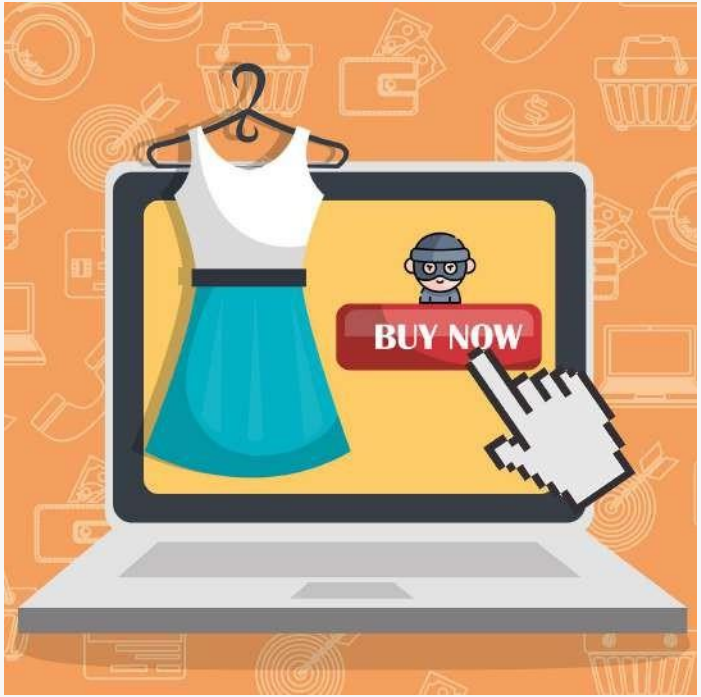
No legitimate company asks for money in the name of bond or security deposits in advance.

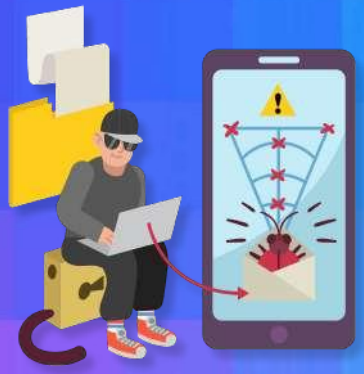
Submit your application through a registered website only. Never pay in advance.

ALL JOB OFFERS THAT REQUIRE YOU TO PAY HUGE AMOUNTS IN ADVANCE ARE FRAUDULENT.

PAYMENT FRAUD USING FAKE E-COMMERCE SITES

In This type of fraud a cybercriminal comes up with a fake merchant website which looks similar to that of a legitimate business. The culprit then goes ahead and places fake offers on expensive/branded products at very hard-to-resist prices and popularizes the site through social media Ads. Victim clicks on such links to buy products, with payment being done through UPI or online banking and will get cheated.





Modus Operandi

1. Fraudsters host fake online shopping portals with the intention to cheat people which offer hard-to-resist prices. Such fake websites are popularized through social media Ads.
2. Fraudsters use the link to target social media users.
3. Victim clicks on one such link to buy a mobile phone, with payment being done through UPI.
4. No product/Cheap Product will be delivered to the victim and he/she loses money.

Pay attention to the address bar and check the domain name.

Look for customer feedback on the internet, research about the website.

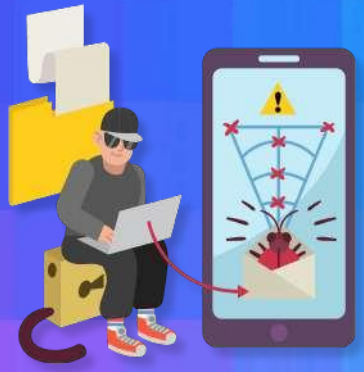
Don’t be fooled by logos, it can be replicated easily.

Check the customer grievance redressal policy and contact details.

ALWAYS RELY ON POPULAR SITES AND CHECK REVIEWS BEFORE MAKING A CHOICE.

Scams by Gaining Remote Access to Devices

The scammers target individuals by impersonating trusted entities, like banks or tech support. Victims are tricked into downloading remote connect apps, granting scammers remote access to their devices. This enables theft of sensitive information, including login credentials and banking details, leading to unauthorized transactions or complete account takeover.



Modus Operandi

1. Scammers call, message, or reach out via social media claiming to be from a trusted company.
2. They create a sense of urgency, stating critical issues with your device or account require immediate fixing.
3. "Fix" with Remote App: They offer to resolve the problem using a specific app, urging you to download and install it.
4. Once installed, they convince you to grant the app remote access to your device.
5. Fraudster persuades the victim to make a small amount like Rs.50/- , then the fraudster watches the transaction activity through remote app.
6. Later, Using stolen credentials, fraudster carry out unauthorized transactions or take control of your accounts.

Never use money transactions when using app like Team Viewer, Any desk in your device

Be cautious with app permissions, especially remote access.

HELPFUL TIPS

Verify caller identity through official channels.

Use strong passwords and enable two-factor authentication.

NEVER INSTALL APPLICATIONS DIRECTED BY OTHERS. THESE APPLICATIONS MAY STEAL YOUR BANKING CREDENTIALS THROUGH REMOTE DESKTOP ACCESS.

IF YOU ARE A FINANCIAL FRAUD VICTIM
IMMEDIATELY REPORT IT OVER

TOLL FREE NUMBER

1930

9497980900

cybercrime.gov.in

Thank You

Kerala Police