Online Job and Investment Scams

Fake work-from-home jobs, task scams and 'guaranteed return' schemes - how to spot them early.

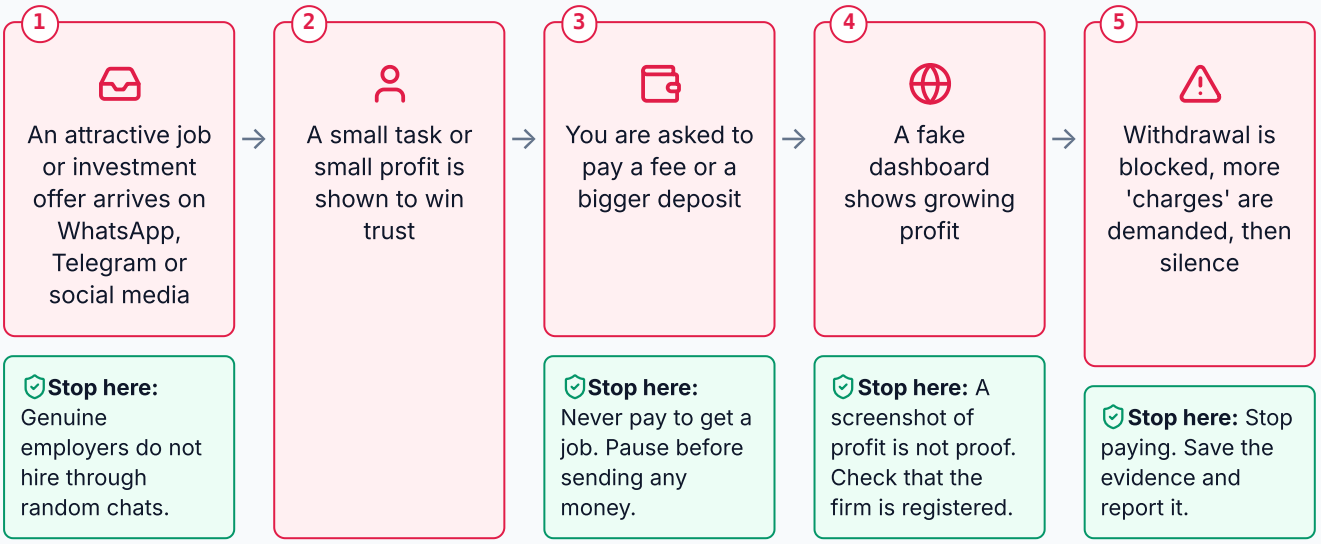
Lost money in an online fraud? Call 1930 right away and report at cybercrime.gov.in.

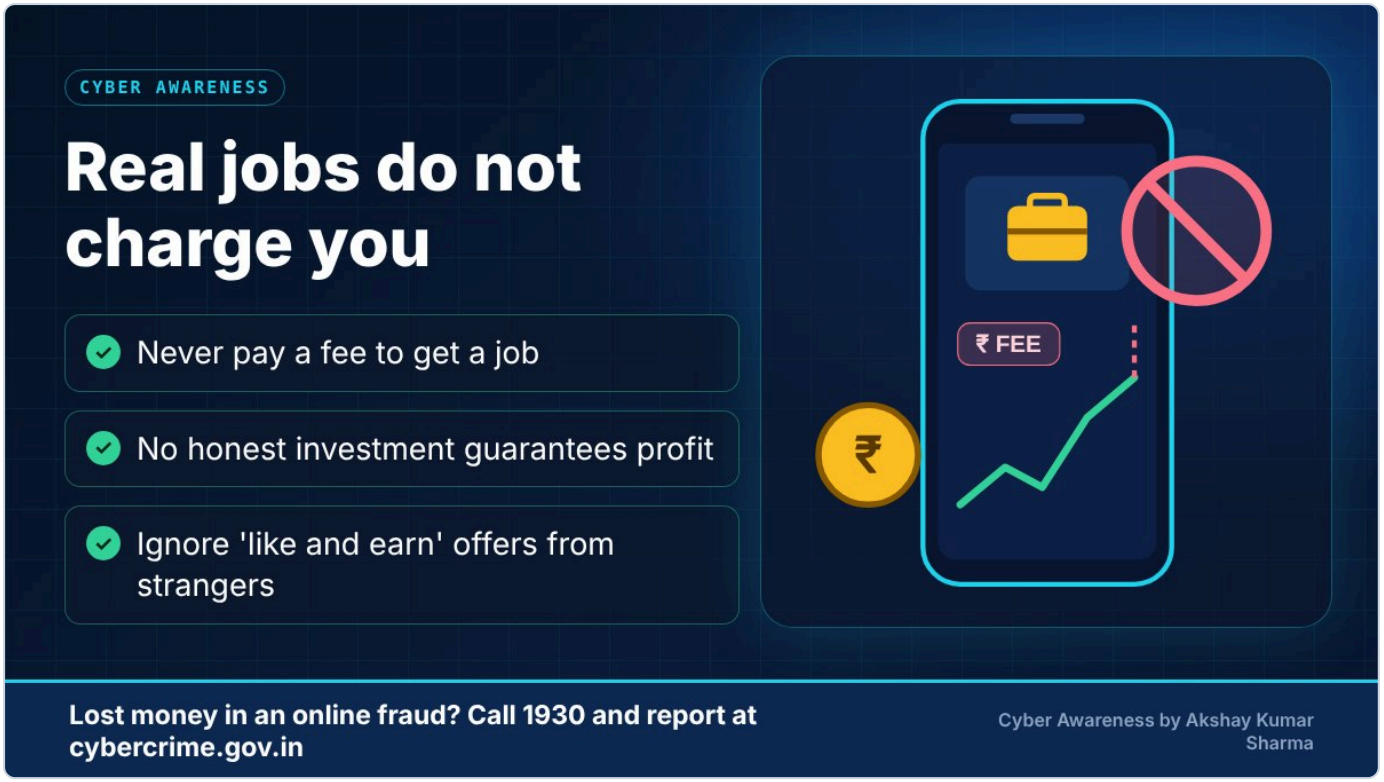
What it is

These scams promise easy money: a part-time job for a few minutes a day, rewards for liking videos, or investments with assured high returns. They often begin on messaging apps or social media. Victims are first shown small 'profits' to build trust, then pushed to deposit larger and larger amounts that they cannot withdraw.

How it works - and where you can stop it

Red boxes show what the attacker does. Green boxes show where you can break the chain.





Common warning signs

- ⚠ Job offers from unknown numbers on WhatsApp or Telegram, with high pay for very simple tasks.
- ⚠ You are asked to pay a 'registration', 'security' or 'processing' fee before you can work or withdraw.
- ⚠ Guaranteed or unusually high returns with little or no risk.
- ⚠ Pressure to deposit more to 'unlock' earlier profits.
- ⚠ No verifiable company details, or an unregulated platform or app link sent in a chat.

Practical prevention tips

- A genuine employer does not charge you to give you a job. Verify the company on its official website.
- Treat 'guaranteed returns' as a red flag. Check that an investment firm or advisor is registered with the relevant regulator.
- Do not join investment groups or install apps shared by strangers.
- Never make payments to personal accounts for jobs or investments.
- Discuss any big financial decision with someone you trust before paying.

Risky habit vs safe habit

RISKY	SAFE
✕ Pay a 'registration fee' for a job	✓ Remember: real jobs do not charge candidates
✕ Trust 'guaranteed' high returns	✓ Know that no honest investment guarantees profit
✕ Join 'tips' groups run by unknown numbers	✓ Use only registered, regulated intermediaries
✕ Do 'like and earn' tasks offered by strangers	✓ Ignore part-time task offers from unknown people

What to do if it happens

1. Stop sending money, even if you are promised that the next payment will release your funds.
2. Call the cyber crime helpline 1930 immediately - reporting quickly gives the best chance of stopping the transfer.
3. Also file a complaint on the National Cyber Crime Reporting Portal (cybercrime.gov.in).
4. Inform your bank or payment app right away and ask them to block the card, account or UPI ID involved.
5. Keep screenshots, transaction IDs, phone numbers, UPI IDs and chat history. Do not delete anything.
6. Change passwords of affected accounts and do not share OTPs or PINs with anyone who calls you afterwards offering to 'recover' your money.

Official reporting resources

- Cyber crime helpline 1930 (for financial cyber fraud) - 1930
- National Cyber Crime Reporting Portal (cybercrime.gov.in) - https://cybercrime.gov.in/
- Reserve Bank of India - public awareness - https://www.rbi.org.in/

Never share your banking password, OTP, UPI PIN, card CVV or full card number with anyone - not even someone claiming to be from your bank, police or a government office. This website will never ask for them.

This website is an educational resource. It is not an official government reporting portal or an emergency response service. If you are a victim of cyber fraud, report it through the official channels listed on each page.
Akshay Kumar Sharma - https://www.youtube.com/@cybersecwithakshay