



HAND BOOK ON CURRENT CYBER CRIMES

A Infographic Explanation of Cyber Crimes

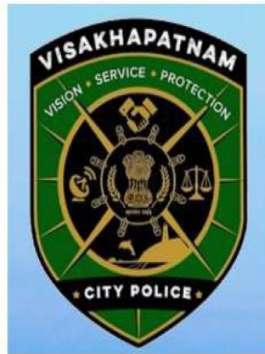


JOINT INITIATIVE OF VIZAG CITY POLICE
&
VIZAG SECURITY COUNCIL



Social Media Channels of Visakhapatnam City Police

FOLLOW



-  <https://www.youtube.com/@vizagcitypolice/>
 -  <https://www.facebook.com/visakhapatnamcitypolice/>
 -  <https://twitter.com/vizagcitypolice>
 -  <https://www.instagram.com/vizagcitypolice/>
 -  <https://whatsapp.com/channel/0029vaOHOjjHQbSDllrlat1p>
- web://https://sancharsaathi.gov.in

FOREWORD



In the digital age, where technology permeates every aspect of our lives, the threat of cybercrime looms larger than ever before. As we embrace the conveniences and opportunities offered by the internet, we must also confront the inherent risks posed by malicious actors seeking to exploit vulnerabilities for personal gain affecting individuals, businesses, and societies worldwide.

This "Infographic explanation on Cyber Crimes" serves as a crucial resource in our collective effort to combat cyber threats and protect ourselves in an increasingly interconnected world. By examining real-world case studies and emerging trends, it equips readers with the knowledge and awareness needed to recognize, prevent, and respond to cyber threats effectively.

Beyond the immediate financial and emotional toll on victims, cybercrime poses a systemic threat to our collective security, economic stability, and societal well-being. From ransomware attacks targeting critical infrastructure to social engineering schemes exploiting human psychology, the tactics employed by cybercriminals continue to evolve in sophistication and scale.

As per statistic of NCRP Portal says that, so far in Visakhapatnam city around 12 thousand victims were cheated under various Cyber frauds reported in National Cyber Crime reporting Portal /1930 (CFCFCRMS, Citizen Financial Cyber Frauds Reporting and Management System) and loss of total amount Rs. 85,51,90,001/- in that Rs. 8,90,29,920/- was kept hold by the I4C.

Awareness is the first line of defense against cybercrime. By understanding the tactics employed by cybercriminals and staying informed about the latest cybersecurity best practices, individuals and organizations can significantly reduce their risk exposure and safeguard their digital assets.

Vizag City Police and Visakhapatnam Security Council efforts underscore the importance of education, vigilance, and collaboration in addressing the complex challenges posed by cyber threats.

Together, we can build a more secure and resilient cyber ecosystem—one where trust, integrity, and innovation thrive, and where the benefits of technology are enjoyed by all.

Dr.A.Ravi Shankar, IPS.,
Commissioner of Police &
Addl. District Magistrate
Visakhapatnam Metropolitan City
Andhra Pradesh

INDEX

S.No	TRENDING FRAUD POSTERS	Pages
1.	Fake stock market-Investment fraud	1-3
2.	Crypto Currency-Investment fraud	4-5
3.	Part time Job/Tasks, (Hotel reviews, Google Map reviews, movie ticket ratings and reviews, Ratingsto Online marketing Garment setc...)	6-8
4.	Fedex fraud	9-10
5.	KYC update link Fraud (Credit Card Redeem / PAN / AADHAR Card Updation)	11-21
6.	Fake Job Fraud (Naukari.com, Shine.com etc)	22-23
7.	Google Search Customer Care Numbers / Phishing	24-26
8.	Social Media Frauds (Cyber Stalking/ Sexual Harassment / Morphing Photos)	27-30
9.	Olx Fraud (Buying / Selling Goods)	31-32
10.	Fake Loan Fraud (India Bulls, Bajaj Finance etc..)	33-34
11.	House Rental Scam (99.acress/Housing.com/ Magic Bricks/)	35-36
12.	Lottery Fraud/Gift Fraud/Matrimonial Fraud	37-42
13.	Instant Loan Apps Harassment	43-48
14.	Electricity Bill Payment Frauds	50
15.	Mesho/Amazon gift vouchers Fraud	51
16.	Whats app Impersonation	52-53
17.	Sextortion (Honey Trap)	58
18.	AEPS	59-60
19.	BEC (Businesses Mail compromise) Spoofing & Snooping	61-63
20.	Sanchar Saathi	64-65
21.	Mobile Security	66
22.	Cyber Hygiene	67
23.	Cyber Crime Punishment Sections	68

BEWARE OF INVESTMENT FRAUDS



- ❌ Don't invest money believing words of fraudster over any app.

- ❌ Don't click the links and download apps for investment.

- ❌ Don't invest in tips given by unknown people on social media.

**VISAKHAPATNAM
CITY POLICE**



**CYBER FRAUD
REPORTING NUMBER 1930**
www.cybercrime.gov.in

అన్వేషణమెంట్ మోసాలతో జాగ్రత్త



- ✘ పెట్టుబడులు పెడితే అధిక లాభాలు పొందవచ్చంటూ మోసగాళ్ల మాటలు నమ్మి డబ్బు పెట్టుబడి పెట్టకండి.
- ✘ పెట్టుబడి కోసం తెలియని లింక్లను క్లిక్ చేసి యాప్లను డౌన్లోడ్ చేయవద్దు.
- ✘ సోషల్ మీడియా లో తెలియని వ్యక్తులు ఇచ్చే టిప్స్ తో పెట్టుబడులు పెట్టకండి.

విశాఖపట్నం
సిటి పోలీస్



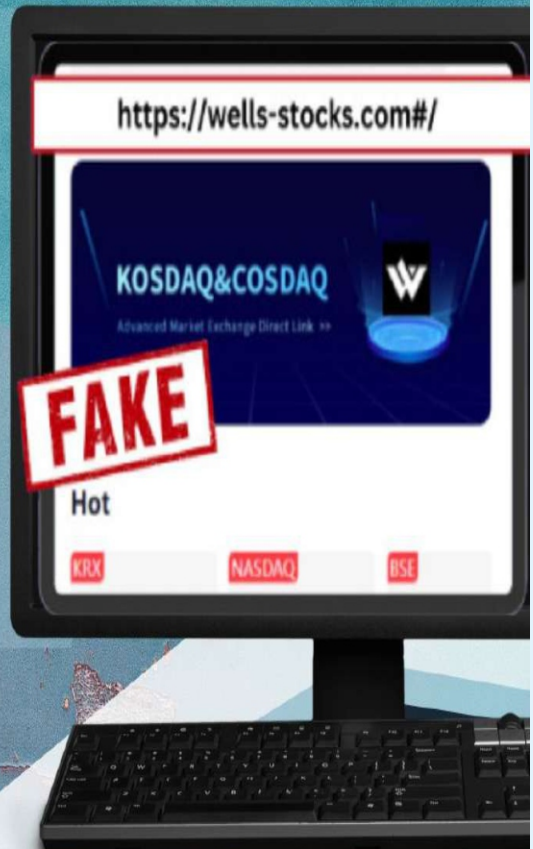
సైబర్ ఫిర్యాదుల కోసం
కాల్ చేయండి **1930** కి
www.cybercrime.gov.in



FAKE TRADING WEBSITE

SEBI ADVISORY

Beware fake stock schemes on social media claiming SEBI approval. Be cautious



DIAL 1930

CRYPTO CURRENCY SCAM

How its done

- » If we download fake mobile apps created by cyber criminals, they will take control of our mobile phones.
- » Cybercriminals are sending links to fake websites to our e-mail, WhatsApp. If you open them, they will send you some more links called online payment.

Safety tips

- » Do not click on suspicious links in your e-mail.
- » Do not really trust the links that come with tips regarding cryptocurrency investments.
- » If there are typos, strange logos and colors on the websites, it should be identified as a fake website.

**VISAKHAPATNAM
CITY POLICE**



**CYBER FRAUD
REPORTING NUMBER 1930**
www.cybercrime.gov.in

క్రిష్టా కరెన్సీ స్కామ్స్ తో జాగ్రత్త

క్రిష్టా మోసం ఏలా జరుగుతుంది

- >> సైబర్ సేరగాళ్లు సృష్టించిన ఫేక్ మొబైల్ యాప్లను డౌన్లోడ్ చేస్తే మీ మొబైల్ వాళ్ల కంట్రోల్లోకి వెళ్లిపోతుంది
- >> నకిలీ వెబ్సైట్ లింకులు మీ ఈ-మెయిల్, వాట్సాప్ కి సైబర్ సేరగాళ్లు పంపుతారు, వాటిని ఓపెన్ చేస్తే అన్లైన్ పేమెంట్ చేయలి అంటూ మరికొన్ని లింకులు పంపుతారు

ఏలా జాగ్రత్త వడాలి

- >> మీ ఈ-మెయిల్ లేదా వాట్సాప్ కి వచ్చే అనుమానస్పద లింకులు క్లిక్ చేయకండి
- >> క్రిష్టా కరెన్సీ లో ఏలా డబ్బులు సంపాదించాలో టిప్స్ చెప్తామంటు వచ్చే లింక్స్ ని నమ్మకండి
- >> వెబ్సైట్లో అక్షరదోషాలు, రంగులు, వింత లోగులు ఉంటే అది ఫేక్ వెబ్సైట్ అని గుర్తించండి

విశాఖపట్నం
సిటి పోలీస్

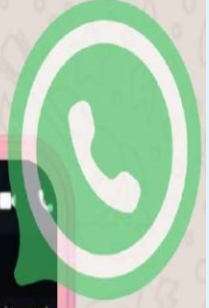
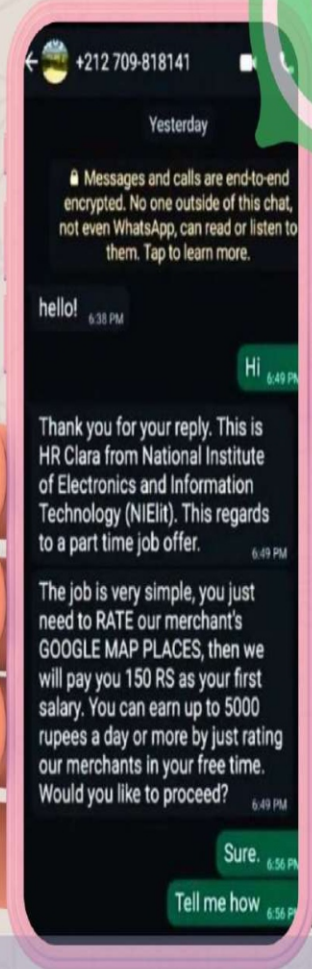


సైబర్ ఫిర్యాదుల కోసం
కాలే చేయండి **1930** కి
www.cybercrime.gov.in



PART TIME JOB SCAM

సైబర్ నేరగాళ్లు
నకిలీ పార్ట్ టైమ్
జాబ్ ఆఫర్లతో
ప్రజలను నమ్మించి
మోసం చేస్తున్నారు

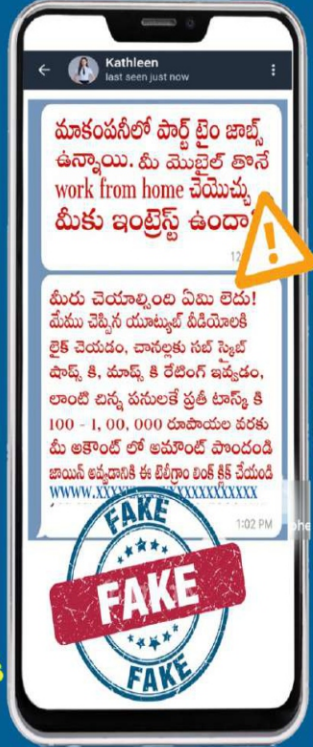


DIAL 1930

టిలీగ్రాంలో పార్ట్ టైం జాబ్ టాస్కులు నమ్మకండి

- ▶ టిలీగ్రాం ఆప్ లో టాస్క్ కంప్లీట్ చేసి స్కీన్-షాట్ పెడితే మీ అకౌంట్ లో డబ్బు వేస్తాం అంటారు
- ▶ మొదట చిన్న చిన్న అమౌంట్స్ మీ బాంక్ ఖాతాలో వేసి మిమ్మల్ని నమ్మిస్తారు.
- ▶ తరువాత టాస్కులకి డబ్బు కట్టి జాయిన్ అవ్వాలని టాస్క్ పూర్తి చేస్తే లక్షల్లో డబ్బు ఇస్తామని చెప్తారు.
- ▶ మీ నుండి పలురకాలుగా డబ్బు కట్టించుకుంటారే కానీ తిరిగి చెల్లించరు.

టిలీగ్రాంలో టాస్కుల జోలికిపోకండి - అప్రమత్తంగా ఉండండి



VISAKHAPATNAM CITY POLICE



టెలిగ్రాం లో పార్ట్-టైం జాబ్ టాస్క్ లు నమ్మకండి

ఇదొక కొత్తరకం సైబర్ మోసం

- ▶ పార్ట్ టైం జాబ్ కి సెలెక్ట్ అయ్యారని టెలిగ్రాం లోకి రమ్మని మీ మొబైల్ కి లింక్ పంపిస్తారు
- ▶ వారు చెప్పిన యూట్యూబ్ విడియోస్ కి లైక్ చెసి, చానల్ కి సబ్ స్క్రైబ్ చేసి స్ట్రీమ్ షాట్ పెట్టమని ఇలా రక రకాల టాస్క్ లు చెప్పారు
- ▶ మిమ్మల్ని నమ్మించడానికి మొదట చిన్న మొత్తం లో మీ అకౌంట్ లో డబ్బులు వేసి నమ్మిస్తారు
- ▶ మీరు నమ్మాక ప్రీపేయిడ్ టాస్క్ అని లక్షల్లో లాభం ఇస్తామని మొదట డబ్బులు కట్టాలని మీతో ఆదిక మొత్తం లో డబ్బులు కట్టిస్తారు
- ▶ మీకు లక్షల్లో లాభాలు వచ్చినట్టు నకిలీ స్క్రీన్లు, చూపించి ముందు టాక్స్ కట్టాలని రక రకాల అడ్వాన్స్ లు కట్టాలని మీతో కట్టించుకుంటారు
- ▶ కానీ ఎప్పటికీ వారు మాత్రం మీకు డబ్బులు వేయరు
- ▶ ఇటీవల చాలా మంది ఇలా లక్షలలో మోసపోతున్నారు. అప్రమత్తం గా ఉండండి.



VISAKHAPATNAM CITY POLICE

FedEx Scam: The Modus Operandi



Your package could not be delivered. Press #1 to know more

Automated phone call from Fedex

Your package had prohibited items. Matter is a police case now



Customer care agent talks to you

Come in person or record a statement over Skype



Cop says you must record a statement immediately

These are RBI rules



Asks you to transfer money to 'verify' if there's any suspicious transaction

Dial 1930

నకిలి FedEx కొలియర్ బెదిలింపు ఫోన్ కాల్ తో అప్రమత్తంగా ఉండండి!

మీరు పంపిన పార్సెల్ లో ద్రగ్స్ ఉన్నాయి
ముంబాయి పోలీస్ మీకు ఫోన్ చేస్తారు



నకిలి FedEx

మీ మీద ద్రగ్స్ కేస్ లిజిస్టర్ అయ్యింది
SKYPE కాల్ చేసి మీ స్కైప్ లోంచి రికార్డు
చేస్తుంది



నకిలి ముంబాయి పోలీస్/నార్కోటిక్ డిపార్ట్ మెంట్

RRB రూల్ ప్రకారం ద్రగ్స్ పార్సెల్
చేసినందుకు ONLINE ద్వారా
మా అకౌంట్ కు రూ. 25 లక్షలు
కట్టించి లేదంటే అరెస్ట్ చేస్తాం



ఫెడెక్స్ కొలియర్ పేరుతో మీరు పంపిన పార్సెల్ లో ద్రగ్స్ ఉన్నాయని,
మీరు పంపించ లేదు అన్నా మీ పేరుతో పార్సెల్ పంపించారని మిమ్మల్ని బుకాయించి,
ముంబాయి పోలీసులు కేసు లిజిస్టర్ చేసారని, మీతో మాట్లాడుతారని చెప్తారు

మీరు నమ్మితే ఫోన్ లోనే స్కైప్ ద్వారా నార్కోటిక్ డిపార్ట్ మెంట్ అని విచారణ చేసి
డబ్బులు కడితే వదిలేస్తామని బెదిలించి మీతో లక్షల్లో డబ్బులు కట్టించుకొని
మొసం చేస్తారు.

నార్కోటిక్ డిపార్ట్ మెంట్, పోలీస్, సి.బి.ఐ.
వంటి ప్రభుత్వ సంస్థలు మీకు ఫోన్ చేసి విచారణ జరపవు
విచారణ పేరుతో డబ్బులు అడగవు
అప్రమత్తంగా ఉండండి!

CYBER CRIME POLICE STATION
VISAKHAPATNAM CITY

BEWARE SENIOR CITIZENS

Digital life certificate scam

Phone calls are made to pensioners under the pretext to update your Digital Life Certificate. Don't share any personally identifiable information like Aadhar Number, PAN number or Banking Information



Always Remember

- Pension Distribution Authorities will never call pensioners
- They never request pensioners to share their sensitive banking information

**VISAKHAPATNAM
CITY POLICE**



**CYBER FRAUD
REPORTING NUMBER 1930**

www.cybercrime.gov.in

సీనియర్ సిటిజన్స్ జాగ్రత్తగా ఉండండి

డిజిటల్ లైఫ్ సర్టిఫికేషన్ మోసాలతో జాగ్రత్త

మీ డిజిటల్ లైఫ్ సర్టిఫికేట్ను అవ్వడం చేయాలి, లేదంటే రద్దు అవుతుంది అని సైబర్ నేరగాళ్ళు పెన్షనర్లకు కాల్స్ చేస్తున్నారు. అలాంటి నకిలీ కాల్స్ కి ఆధార్ నంబర్, పాన్ నంబర్ లేదా బ్యాంకు సమాచారాన్ని షేర్ చేయకండి.



ఎల్లప్పుడూ గుర్తుంచుకోండి

- పెన్షన్ పంపిణీ అధికారులు పింఛనుదారులకు ఎప్పుడు కాల్ చేయరు
- మీ బ్యాంకు సమాచారాన్ని షేర్ చేయమని పెన్షన్ అధికారులు మిమ్మల్ని అడగరు

విశాఖపట్నం
సిటి పోలీస్



సైబర్ ఫిర్యాదుల కోసం
కాల్ చేయండి **1930** క్రి

www.cybercrime.gov.in

నేకీలే కాల్స్ తో నీనియర్ సిటిజన్స్ జార్జత్త



బ్యాంకు అధికారులమని చెప్పి సైబర్ నేరగాళ్లు మిమ్మల్ని నమ్మించి మీ డెబిట్/క్రెడిట్ కార్డు వివరాలు అడగవచ్చు. జార్జత్త గా ఉండండి.

► మీ ఓటీపీ, డెబిట్ కార్డు, వ్యక్తిగత సమాచారాన్ని ఎలాంటి పరిస్థుల్లోనూ ఎవరికి చెప్పకండి.

► మీ వ్యక్తిగత వివరాలను దుర్వినియోగం చేస్తారు, మీ ఖాతా లో నగదు కూడా దోచేస్తారు



విశాఖపట్నం
సిటి పోలీస్



సైబర్ ఫిర్యాదుల కోసం
కాల్ చేయండి **1930** కి
www.cybercrime.gov.in

BEWARE OF FAKE BANK PHONE CALLS



- Through a short message circular, the fraudster's can steal money from your banks
- Beware of fake calls like Activating and deactivating debit card, credit card and KYC etc
- Never share your Account details, OTP, debit card details or any other confidential information through phone calls

**VISAKHAPATNAM
CITY POLICE**



**CYBER FRAUD
REPORTING NUMBER 1930**

www.cybercrime.gov.in

బ్యాంక్ అధికారులనుంటు వచ్చే నకిలీ కార్డ్ తో జాగ్రత్త



- ఒక చిన్న మెసేజ్ తో మీ కార్డ్ లో ఉన్న నగదు మొత్తం దోచెస్తారు
- డెబిట్ కార్డు యాక్టివేషన్ / డియాక్టివేషన్ అని చెప్పే నకిలీ కార్డ్స్ ని గ్రహించండి
- ఎలాంటి పరిస్థితులోను మీ ఓటీపీ, డెబిట్ కార్డు, వ్యక్తిగత సమాచారాన్ని ఎవరితోను షేర్ చేయకండి

విశాఖపట్నం
సిటి పోలీస్



సైబర్ ఫిర్యాదుల కోసం
కాల్ చేయండి **1930** కా
www.cybercrime.gov.in

“Don’t take *the bait*”

Clicking Unknown Links and
Entering Your Bank or Card Details
can empty your bank account



**VISAKHAPATNAM
CITY POLICE**

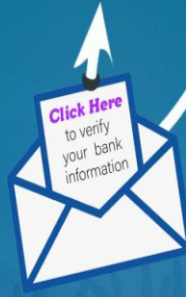


**CYBER FRAUD
REPORTING NUMBER 1930**

www.cybercrime.gov.in

“సైబర్ నేరగాళ్లకి ఎర అవ్వకండి”

తెలియని లింక్లు క్లిక్ చేయడం మరియు
మీ బ్యాంక్ లేదా కార్డ్ వివరాలు నమోదు చేయడం
ద్వారా బ్యాంక్ ఖాతాను సైబర్ నేరగాళ్లు ఖాళీ చేయవచ్చు



విశాఖపట్నం
సిటి పోలీస్



సైబర్ ఫిర్యాదుల కోసం
కాల్ చేయండి **1930** క్రి
www.cybercrime.gov.in

BEWARE OF PHISHING SCAMS



BEWARE OF UNSOLICITED MESSAGES



- Attachements
- Links
- Login pages

Think before you click any link
attachments

If in doubt **flag** or **report** as phising

**VISAKHAPATNAM
CITY POLICE**



**CYBER FRAUD
REPORTING NUMBER 1930**
www.cybercrime.gov.in

ఫిషింగ్ స్కామ్స్ తో జాగ్రత్త



అనుచిత మెసేజీలతో జాగ్రత్త



- అటాచ్మెంట్స్
- లింక్స్
- లాగిన్ పేజెస్

ఏదైనా లింక్ అటాచ్మెంట్స్ క్లిక్ చేసే ముందు ఆలోచించండి

ఎటువంటి సందేహాలు ఉన్న ధ్లాగ్ చేయండి

లేదా ఫిషింగ్ అని రిపోర్ట్ చేయండి

విశాఖపట్నం
సిటి పోలీస్

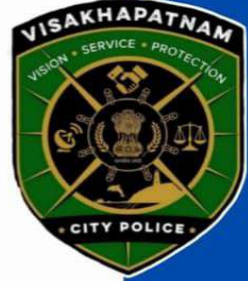


సైబర్ ఫిర్యాదుల కోసం
కాల్ చేయండి **1930** కి
www.cybercrime.gov.in



+917797806097 ✓

Thursday, 10 November



Dear User Your SBI Netbanking has been suspended. Today due to E-KYC failure. Please update your PAN CARD no immediately via-link <http://sruv-hom.firebaseio.com/ekycsbi>

**SCAM
ALERT**



మీ SBI INTERNET BANKING బ్లాక్ అయిందని PAN CARD అప్డేట్ చెయ్యమని వచ్చే మెసేజులు నమ్మకండి.

సైబర్ మోసగాళ్లు పంపించే ఇలాంటి మెసేజెస్ లో ఉండే లింక్స్ ని క్లిక్ చెయ్యకండి, ఎలాంటి బ్యాంకు వివరాలు తెలియచేయకండి.

సైబర్ క్రైం, విశాఖపట్నం సిటీ

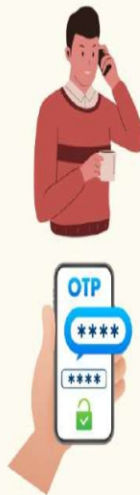


MORAL STORY

They called
from bank

He shared
OTP

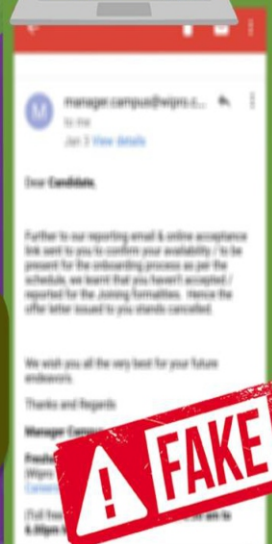
Bank account
emptied



Moral : Never share your OTP

BEWARE OF JOB SCAMS

- You didn't apply ; they contacted you
- Asking for money
- Asking for confidential information
- Without interview you get job



Job offers without an interview



Being asked for money



Poorly-written job adverts



Suspicious contact details

**VISAKHAPATNAM
CITY POLICE**

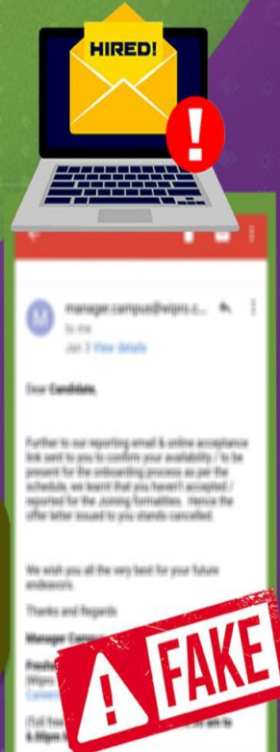


**CYBER FRAUD
REPORTING NUMBER 1930**

www.cybercrime.gov.in

జాబ్ స్కామ్స్ తో జాగ్రత్త

- మీరు అప్లై చేయలేదు ; వారు మిమ్మల్ని సంప్రదించారు
- మిమ్మల్ని డబ్బులు అడుగుతారు
- మీ వ్యక్తిగత సమాచారాన్ని (రహస్య సమాచారం) అడుగుతారు
- ఇంటర్వ్యూ లేకుండానే మీకు ఉద్యోగం వస్తుంది



			
ఇంటర్వ్యూ లేకుండా ఉద్యోగ ఆఫర్లు	డబ్బులు అడగటం	ఉద్యోగ పత్రావలీలు ఫోన్ గా ఉండటం	అనుమానాస్పద వివరాలు

విశాఖపట్నం
సిటి పోలీస్



సైబర్ ఫిర్యాదుల కోసం
కాలే చేయండి **1930** క్ర
www.cybercrime.gov.in



VISAKHAPATNAM CITY POLICE



BEWARE OF FAKE CUSTOMER CARE NUMBERS

THE CYBER CRIMINALS ARE WAITING BEHIND EVERY
FAKE CUSTOMRE CARE NUMBER IN GOOGLE

CYBER FRAUD
REPORTING NUMBER **1930**

www.cybercrime.gov.in



విశాఖపట్నం సిటి పోలీస్



నకిలీ కస్టమర్ కేర్ నంబర్లతో జాగ్రత్త

గూగుల్ లో వెతికే కస్టమర్ కేర్ నంబర్ల చాటున సైబర్ నేరగాళ్లు పొంచి ఉన్నారు జాగ్రత్త
కస్టమర్ కేర్ నంబర్ల కోసం అధికారిక వెబ్సైట్లో వెతకండి గూగుల్ లో కాదు

సైబర్ ఫిర్యాదుల కోసం
కాల్ చేయండి **1930** కి

www.cybercrime.gov.in



Google

Do not search for Customer Care Number

ప్రజలకు విజ్ఞప్తి

మీరు గూగుల్ లో వెతికే కస్టమర్ కేర్ నెంబర్ చాటున సైబర్
నేరగాళ్ళు పొంచి ఉన్నారు జాగ్రత్త.
కస్టమర్ కేర్ నెంబర్ కోసం సంబంధిత అధికారిక వెబ్సైటులోనే
వెతకండి, గూగుల్ కాదు.

Beware of strangers in social networking sites



Don't share your sensitive information with unknown people on social networking websites

Cybercriminals can misuse your information or blackmail you for money

**VISAKHAPATNAM
CITY POLICE**



**CYBER FRAUD
REPORTING NUMBER 1930**

www.cybercrime.gov.in

సోషల్ మీడియా సైట్లలో అపరిచిత వ్యక్తులతో జాగ్రత్త

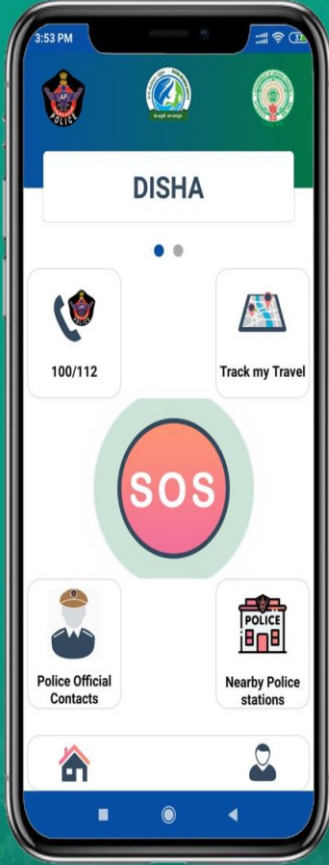


సోషల్ నెట్వర్కింగ్ వెబ్ సైట్ లలో తెలియని వ్యక్తులతో మీ సున్నితమైన సమాచారాన్ని షేర్ చేయకండి
 సైబర్ నేరగాళ్లు మీ సమాచారాన్ని దుర్వినియోగం చేయవచ్చు
 లేదా డబ్బులు కోసం మిమ్మల్ని బ్లాక్ మెయిల్ చేయవచ్చు

విశాఖపట్నం
 సిటి పోలీస్



సైబర్ ఫిర్యాదుల కోసం
 కాల్ చేయండి **1930** క్రి
www.cybercrime.gov.in



మీ రక్షణ కోసం విద్యార్థినులు, యువత, మహిళలు

దిశ

మొబైల్ యాప్ డౌన్లోడ్ చేసుకోండి



100 112 192

అపదలో ఉన్నాము అనిపించినపుడు కాల్ చేయవలసిన సంఖ్యలు



విశాఖపట్నం సిటీ పోలీస్



STOP

#CYBERBULLYING



SAVE

any evidence of the bullying and show an adult

BLOCK

messages or the person.
Do not respond to them in any way.

LOG OFF

the site where the cyberbullying is happening

TALK

to someone you trust

**VISAKHAPATNAM
CITY POLICE**



**CYBER FRAUD
REPORTING NUMBER 1930**
www.cybercrime.gov.in

BEWARE OF Quikr ONLINE SCAMS

- ▶ They cheat by showing the fake ID proof and believing that the price is lower than the market.
- ▶ **Do not pay any money in advance before purchasing items on websites like Quikr, Olx**



- ▶ **Be careful, pay after seeing the products face-to-face**



**VISAKHAPATNAM
CITY POLICE**



**CYBER FRAUD
REPORTING NUMBER 1930**

www.cybercrime.gov.in

o|x Quikr ఆన్ లైన్ మోసాలతో జాగ్రత్త

- ▶ మార్కెట్ కంటే తక్కువ ధరకే అని చెప్పి మిమ్మల్ని నమ్మిస్తారు, Fake ID పూర్వ్ చూపించి మోసం చేస్తారు
- ▶ Quikr, Olx లాంటి వెబ్ సైట్ లో వస్తువులు కొనే ముందు ఎటువంటి డబ్బులు ముందుగా చెల్లించకండి



- ▶ జాగ్రత్త గా ఉండండి ,ముఖా-ముఖీ కలిసి వస్తువులు చూసిన తరువాత డబ్బులు చెల్లించండి



విశాఖపట్నం
సిటి పోలీస్



సైబర్ ఫిర్యాదుల కోసం
కాలే చేయండి **1930** కి
www.cybercrime.gov.in

Don't believe the fake campaigns that **Central Government will give loan up to 5 lakhs if you have Aadhaar Card.** It has been clarified that the central government is not implementing any schemes.



- Do not forward such messages to your friends and relatives.
- Never share your personal/financial details with anyone

**VISAKHAPATNAM
CITY POLICE**



**CYBER FRAUD
REPORTING NUMBER 1930**
www.cybercrime.gov.in

ఆధార్ కార్డు ఉంటే కేంద్ర ప్రభుత్వం 5 లక్షల వరకు ఋణం

ఇస్తుంది అనే నకిలీ ప్రచారాలను నమ్మకండి. కేంద్ర ప్రభుత్వం ఎలాంటి పథకాలు అమలు చేయడం లేదని స్పష్టం చేసింది .



- అలాంటి మెసేజ్‌లను మీ స్నేహితులు మరియు బంధువులకు ఫార్వార్డ్ చేయవద్దు.
- మీ వ్యక్తిగత/ఆర్థిక వివరాలను ఎవరితోనూ ఎప్పుడూ పంచుకోవద్దు.

**విశాఖపట్నం
సిటి పోలీస్**

సైబర్ ఫిర్యాదుల కోసం 1930 కి
కాల్ చేయండి
www.cybercrime.gov.in

BEWARE OF **HOUSE RENT SCAMS**



Fraudsters use fake images of beautiful homes, claiming they are available for rent. They collect rental advance and vanish away. When trying to reach, they disconnect the calls or their mobile numbers go unreachable

Do not pay any money in advance while renting a house online

**VISAKHAPATNAM
CITY POLICE**



**CYBER FRAUD
REPORTING NUMBER**

www.cybercrime.gov.in

1930

ఇంటి అద్దె మోసాలతో జాగ్రత్త



అందమైన ఇళ్లను అద్దెకు ఇస్తున్నామని మోసగాళ్లు ఆన్‌లైన్ లో నకిలీ చిత్రాలను చూపించి నమ్మిస్తారు. ముందు అద్దె అడ్వాన్స్ పనులు చేసి కనుమరుగు అయిపోతారు. మీరు కాల్ చేసిన ఆ నెంబర్లు పనిచేయవు.

ఆన్‌లైన్ లో ఇల్లు అద్దెకి తీసుకున్నప్పుడు ముందుగా ఎలాంటి డబ్బులు చెల్లించకండి.

విశాఖపట్నం
సిటి పోలీస్

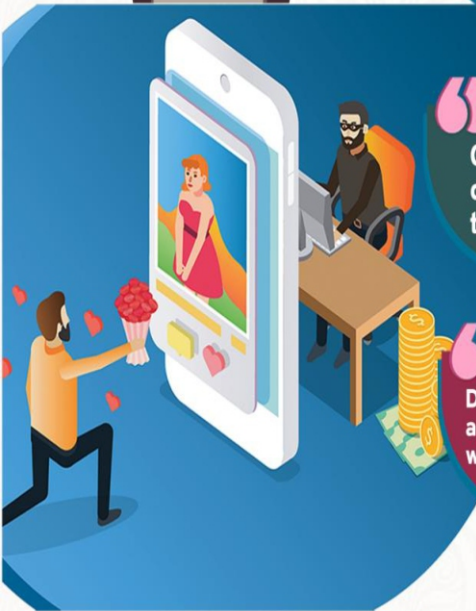


సైబర్ ఫిర్యాదుల కోసం
కాల్ చేయండి **1930** క్రి
www.cybercrime.gov.in

Beware of strangers on matrimonial websites



In online strangers believe that sending valuable gifts



Cyber criminals ask you to please pay custom tax of your valuable gift and they steal your money

Don't get attracted to a matrimonial website and don't deposit money into anyone's account without physical contact approach

**VISAKHAPATNAM
CITY POLICE**



**CYBER FRAUD
REPORTING NUMBER 1930**

www.cybercrime.gov.in

మ్యారేజ్ వెబ్ సైట్ లో అపరిచిత వ్యక్తులతో జాగ్రత్త



“ ఆన్ లైన్ లో అపరిచిత వ్యక్తులు విలువైన బహుమతులు పంపిస్తున్నాం అని నమ్మిస్తారు ”



“ సైబర్ నేరగాళ్లు విలువైన బహుమతి కోసం కస్టమ్స్ సుంకం చెల్లించండి అని మీ యొక్క డబ్బులు దోచేస్తారు ”

“ వివాహ సంబంధిత వెబ్ సైట్ లో వ్యక్తిని చూడకుండా ఆకర్షణకి లోను కాకండి, ఎవరి ఖాతా లోను డబ్బులు వేయకండి ”

విశాఖపట్నం
సిటి పోలీస్



సైబర్ ఫిర్యాదుల కోసం
కాల్ చేయండి **1930** CTA

www.cybercrime.gov.in

ONLINE LOTTERY SCAMS



CONGRATULATIONS!

(1) 100000 Amazon Gift Card

1 is reserved just for you, *Facebook User!*

Step 1: Click the "CONTINUE" button to claim your prize.

Step 2: Enter the correct information on the next page to claim your prize.

2 You only have **4 minutes 14 seconds** to claim your prize!



CONTINUE

Fraudsters will make you believe that they have won a lottery in your name and have huge sums of money.

A link will be sent to give your bank account details, if you click on that link, money will be stolen from your account.

NEVER RESPOND TO FAKE LOTTERY WINNING RELATED CALLS/ SMS

**VISAKHAPATNAM
CITY POLICE**



**CYBER FRAUD
REPORTING NUMBER 1930**

www.cybercrime.gov.in

ఆన్‌లైన్ లాటరీ మోసాలు



CONGRATULATIONS!

(1) 100000 Amazon Gift Card

1 is reserved just for you, *Facebook User!*

Step 1: Click the "CONTINUE" button to claim your prize.

Step 2: Enter the correct information on the next page to claim your prize.

2 You only have **4 minutes 14 seconds** to claim your prize!

amazon

CONTINUE

లాటరీలు, బంపర్ డ్రాలు గెలుచుకున్నారంటూ సైబర్ నేరగాళ్లు మీకు ఆశ చూపిస్తారు. మీ బ్యాంకు ఖాతా వివరాలు ఇవ్వాలని ఒక లింక్ పంపిస్తారు, ఆ లింక్ క్లిక్ చేస్తే మీ అకౌంట్ లో డబ్బులు దోచేస్తారు.

లాటరీ/బంపర్ డ్రాలు వచ్చింది అంటూ వచ్చే మెసేజ్ లేదా కాల్స్ కి స్పందించకండి.

విశాఖపట్నం
సిటి పోలీస్



సైబర్ ఫిర్యాదుల కోసం
కాల్ చేయండి **1930** క్రి
www.cybercrime.gov.in

BEWARE OF LUCKY DRAW SCAMS



- The fraudster provides you the offer of free gifts/prizes saying that you have been selected for the lucky draw

- Ignore the messages/posts received from the unknown numbers



**VISAKHAPATNAM
CITY POLICE**



**CYBER FRAUD
REPORTING NUMBER 1930**
www.cybercrime.gov.in

లక్ష్మీ డ్రా స్కామ్స్ తో జాగ్రత్త



- మీరు భారీ లాటరీ/బహుమతులు గెలుచుకున్నారు అని మోసగాళ్లు మీకు ఇ-మెయిల్ పంపుతారు లేదా ఫోన్ కాల్ చేస్తారు
- ఇలాంటి గుర్తు తెలియని వ్యక్తుల నుండి వచ్చే మెసేజ్/పాస్/కాల్ కి స్పందించకండి



విశాఖపట్నం
సిటి పోలీస్



సైబర్ ఫిర్యాదుల కోసం
కాల్ చేయండి **1930** కి
www.cybercrime.gov.in

FAKE LOAN APPS

Do not download loan apps and don't get attracted with freebies offered to take loans by these fraudulent apps



- ◆ If you are unable to repay , you will be harassed through social media
- ◆ Loan through unknown links/apps can make you victim of cyber fraud

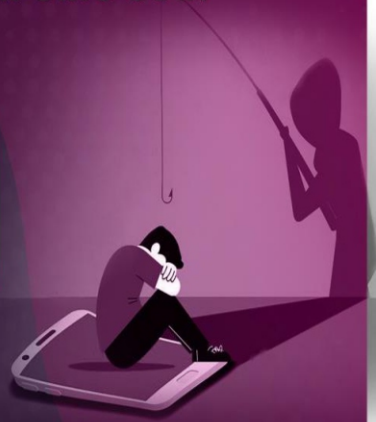
**VISAKHAPATNAM
CITY POLICE**



**CYBER FRAUD
REPORTING NUMBER 1930**
www.cybercrime.gov.in

ఫేక్ లోన్ యాప్స్

లోన్ యాప్ డౌన్లోడ్ చేయకండి మరియు మోసపూరిత ఆఫర్లకు ఆకర్షితులవకండి ఎటువంటి లోన్ తీసుకోకండి.



- ◆ లోన్ తీసుకొని చెలించకపోతే మిమ్ముల్ని సోషల్ మీడియా లో వేధింపులకు గురి చేస్తారు.
- ◆ తెలియని లింకులు/యాప్ల ద్వారా లోన్ తీసుకోకండి , సైబర్ బాధితులు అవ్వకండి

విశాఖపట్నం
సిటి పోలీస్



సైబర్ ఫిర్యాదుల కోసం
కాల్ చేయండి **1930** క్రి
www.cybercrime.gov.in



లోన్ యాప్స్, బుర్రాచీకాలు



ఎటువంటి డాక్యుమెంట్స్ లేకుండా అతితక్కువ వడ్డీకే లోన్ ఇస్తాం అంటారు లోన్ తీసుకున్న తర్వాత మిమ్మల్ని మీ ఫ్యామిలీ ని వేధింపులకు గురి చేస్తారు

2-17-21

రిజర్వ్ బ్యాంకు అనుమతి లేని లోన్ యాప్స్ లో రుణాలు తీసుకోకండి

జాగ్రత్తగా ఉండండి



విశాఖపట్నంసిటి పోలీస్

సైబర్ ఫిర్యాదుల కోసం
కాలే చేయండి **1930** కి
www.cybercrime.gov.in

లోన్ యాప్ లో అడ్డు - మీ ప్రాణాలకే డుడ్డు

జన్ లైన్ లోన్ యాప్ డెన్జిడ్ చేసుకోకండి, లోన్ టీసుకోకండి, వేధింపులకు గురి కాకండి.

లోన్ యాప్ వేధింపులకు గురి అవుతున్నారా ?

- ▶ వేధింపులకు బయపడి ఎటువంటి హాని చేసుకోకండి ధైర్యంగా ఉండండి.
- ▶ నా ప్రమేయం లేకుండా నా ఫోన్ లోన్ యాప్ నిర్వాహకులచే హాక్ కి గురి అయ్యింది, లోన్ యాప్ నిర్వాహకులు మీకు ఏమైనా అసభ్యకరమైన మెసేజీ లు ,కాల్స్ మరియు అసభ్యకరమైన వీడియోస్ వస్తే నమ్మకండి మరియు అపార్థం చేసుకోకండి అని మీ బంధువులు మరియు స్నేహితులకి ముందుగానే తెలియచేయండి.
- ▶ ఇదే సమాచారాన్ని మీ వాట్సాప్ స్టేటస్ ద్వారా అందరికీ తెలియచేయండి.



లోన్ యాప్ వేధింపులకు గురైతే వెంటనే

1930 కి కాల్ చేయండి



**మానసిక వేదనకు గురై ఎలాంటి హాని చేసుకోవద్దు
మిమ్మల్ని సేవ చేయడానికి పోలీస్ శాఖ అండగా ఉంది**

Cybercrime.gov.in వెబ్ సైట్ లో కంప్లైంట్ ని రిజిస్టర్ చేయండి



విశాఖపట్నం సిటి పోలీస్



లోన్ యాప్స్ వాక్కు
వేధిస్తున్నారా ?

అవసరం కోసం ఆన్ లైన్ లో
అప్పు తీసుకున్నారా ?

అప్పు తీర్చిన తర్వాత కూడా
వేధిస్తున్నారా ?



లోన్ యాప్స్
వేధింపులు

విశాఖపట్నం
సిటి పోలీస్



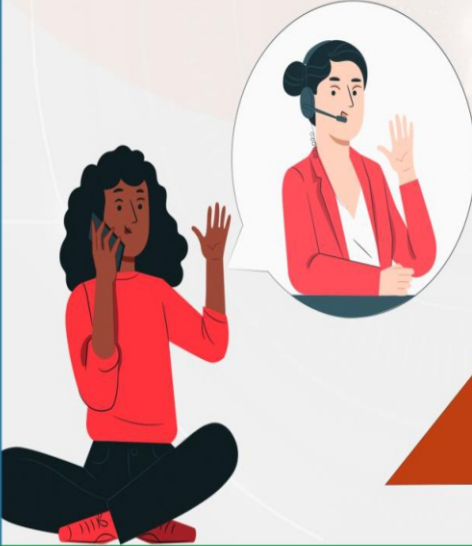
వెంటనే సైబర్ క్రిమ్ నెంబర్ **1930** కి కంప్లెంట్ చేయండి



లోన్ యాప్ ఆగడాలు



మీకు లోన్ అప్లూవ్ అయ్యింది అని అపై చెయ్యకుండానే
 మీకు కాల్స్ లేదా మెసేజ్ వస్తే నమ్మకండి
 మీ వ్యక్తిగత సమాచారాన్ని సేకరించి
 మిమల్ని వేధింపులకు గురిచేస్తారు



లోన్ తీసుకోకండి
 ఇబ్బందుల్లో పడకండి

విశాఖపట్నం సిటి పోలీస్

సైబర్ ఫిర్యాదుల కోసం
 కాల్ చేయండి **1930** కె

www.cybercrime.gov.in



విశాఖపట్నం సిటీ పోలీస్



**“బిల్లు బాకీ ఉంది వెంటనే చెల్లించకపోతే పవర్ కట్ అవుతుంది”
అని మెసేజ్ లు వస్తున్నాయా**

మెసేజ్ లో ఉన్న నెంబర్ కి కాల్ చేస్తే రిమోట్ యాక్సెస్
యాప్స్ ఇన్స్టాల్ చేయించి మీ డబ్బులు దొంగిలిస్తారు
అలాంటి మెసేజ్ లకి స్పందించి - మోసపోకండి

Notification. Dear Customer Your
Electricity power will be
disconnected To night at 9.30 pm
from electricity office.because
your previous month bill was not
update .please immediately
contact with our electricity officer
[6374088845](tel:6374088845) Thank you
15:24

BEWARE!



సైబర్ ఫిర్యాదుల కోసం **1930** కి
కాల్ చేయండి
www.cybercrime.gov.in

follow us!



VisakhapatnamCityPolice



vizagcitypolice.official



VizagCityPolice

మీషో లాటరీ మోసాలతో జాగ్రత్త

meesho



మీషో పేరుతో 12.5 లక్షల రూపాయలను లాటరీ గెలుచుకున్నారు అంటూ రిజిస్టర్డ్ పోస్టు లేదా కాలే వస్తే నమ్మకండి. ఎలాంటి రిజిస్టర్డ్ ఫీజులు చెల్లించకండి. బ్యాంక్ ఖాతా నంబర్, ఖాతాదారు పేరు, పాస్ కార్డ్ వివరాలు, ఆధార్ నంబర్ వంటి వివరాలను ఇవ్వకండి.

సైబర్ నేరగాళ్లు వ్యక్తిగత వివరాలను దుర్వినియోగం చేస్తారు, మీ ఖాతా లో నగదు కూడా దోచేస్తారు. జాగ్రత్త వహించండి.

విశాఖపట్నం
సిటి పోలీస్



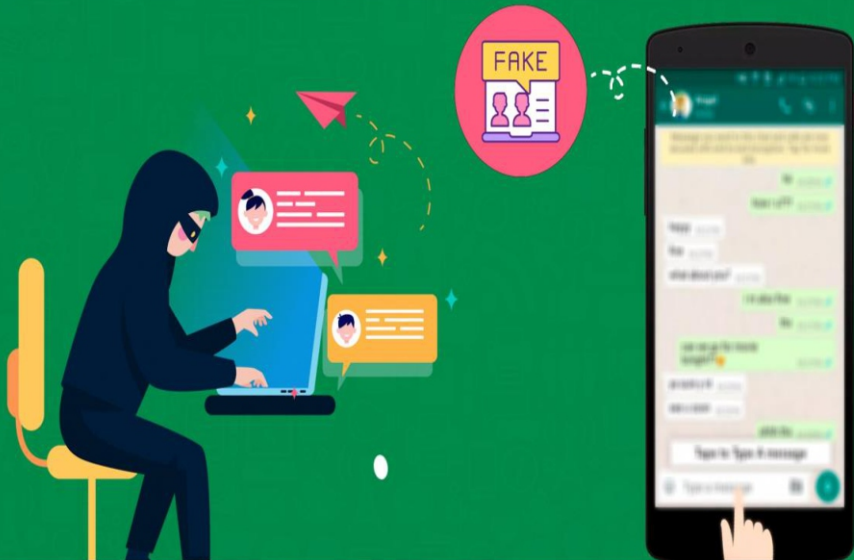
సైబర్ ఫిర్యాదుల కోసం
కాల్ చేయండి **1930** క్రి

www.cybercrime.gov.in

BE ALERT!

Fraudsters may use your friends photograph as WhatsApp DP and ask financial help

Do not believe such messages..Confirm before helping them



**VISAKHAPATNAM
CITY POLICE**

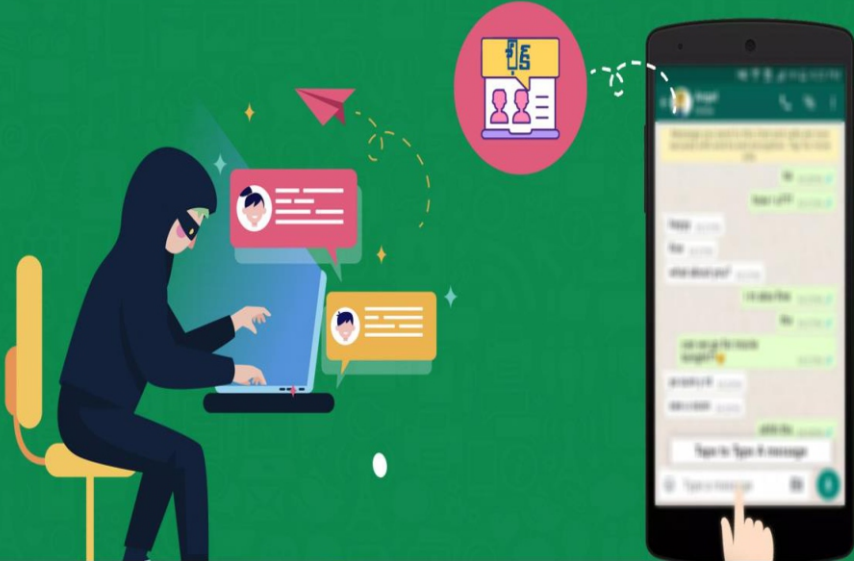


**CYBER FRAUD
REPORTING NUMBER **1930****
www.cybercrime.gov.in

అప్రచుత్తంగా ఉండండి

సైబర్ నేరగాళ్లు మీ స్నేహితుల ఫోటోలు వాట్సాప్ డిపీ గా పెట్టి మిమ్మల్ని ఆర్థిక సహాయం అడగవచ్చు

అలాంటి మెసేజ్లను నమ్మకండి.. సహాయం చేసే ముందు నిరూపించుకోండి



విశాఖపట్నం
సిటి పోలీస్



సైబర్ ఫిర్యాదుల కోసం
కాల్ చేయండి **1930** క్రి
www.cybercrime.gov.in



sextortion



- ▶ Cybercriminals will contact you using a fake account in order to get close to you.
- ▶ Frausters Make a video call and use false nude videos to tempt you into acting the same way.
- ▶ They'll record your nude videos, send you a link and threaten to put them on social media if you don't pay.
- ▶ Be careful with strangers online, don't send your photos/videos to anyone

**Avoid accepting requests from strangers and
Don't post anything in Social media publicly**



**VISAKHAPATNAM
CITY POLICE**



**CYBER FRAUD
REPORTING NUMBER 1930**
www.cybercrime.gov.in

సెక్యూటర్స్



- ▶ సైబర్ నేరగాళ్లు మీకు నకిలీ అకౌంట్స్ తో పరిచయాలు పెంచుకుని దగ్గర అవుతారు
- ▶ వీడియో కాల్ చేసి నకిలీ నగ్న వీడియోలతో మిమల్ని ఎట్రాక్ట్ చేసి మీరు కూడా అలా చేసేలా చేస్తారు
- ▶ మీ నగ్న వీడియోలను రికార్డ్ చేస్తారు , మీకు లింక్ ద్వారా పంపించి డబ్బులు ఇవ్వకపోతే సోషల్ మీడియా లో పెడతాం అని బ్లాక్వైయిల్ చేస్తారు.
- ▶ ఆన్ లైన్ లో అపరిచిత వ్యక్తులతో జాగ్రత్తగా ఉండండి , ఎవరికి మీ ఫోటోస్/వీడియోస్ పంపించకండి

అపరిచితుల రిక్వెస్ట్ లను గ్రహించండి మరియు సోషల్ మీడియా లో పబ్లిక్ గా షేర్ చేయడం మానుకోండి



విశాఖపట్నం సిటి పోలీస్



సైబర్ ఫిర్యాదుల కోసం 1930 ఊర్ కాల్ చేయండి
www.cybercrime.gov.in



HONEY TRAP



- They say that they feel lonely and want new friends. The message is mesmerizing. It is as if you have been deceived if you called believing it to be true
- Scammers trick you, record nude video calls and blackmail you for money.



Do not respond to suspicious messages/calls on social media

**DON'T BE A VICTIM OF
HONEY TRAP**

VISAKHAPATNAM CITY POLICE

**CYBER FRAUD
REPORTING NUMBER 1930**

www.cybercrime.gov.in



హనీ ట్రాప్

- ఒంటరిగా ఫీలవుతున్నా.. న్యూ ఫ్రెండ్స్ కావాలి.. అంటూ ఊరిస్తారు. మెస్సేజ్ చేసేలా మెసేజ్ చేస్తారు. నిజమని నమ్మి కాల్ చేశారో మోసపోయినట్టే
- మోసగాళ్లు మిమ్మల్ని ముగ్గులో దింపి న్యూడ్ వీడియో కాల్స్ రికార్డు చేసి డబ్బుల కోసం బ్లాక్ మెయిల్ చేస్తారు.



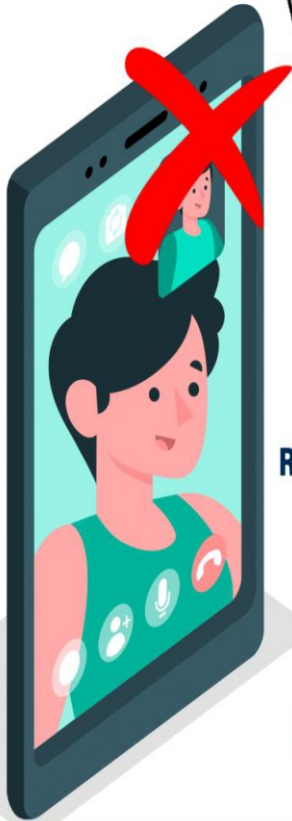
సోషల్ మీడియా లో అనుచునానాస్పద
 మెసేజింగ్/కాల్స్ కి స్పందించకండి
 హనీట్రాప్ బాధితులు అవ్వకండి

విశాఖపట్నం సిటి పోలీస్

సైబర్ ఫిర్యాదుల కోసం **1930** కి
 కాల్ చేయండి
www.cybercrime.gov.in

Stay Alert of **Lured Video Call**

**Never Receive Video call
from Unknown person Dont
Let them Harasse You**



**CYBER FRAUD
REPORTING NUMBER 1930**
www.cybercrime.gov.in



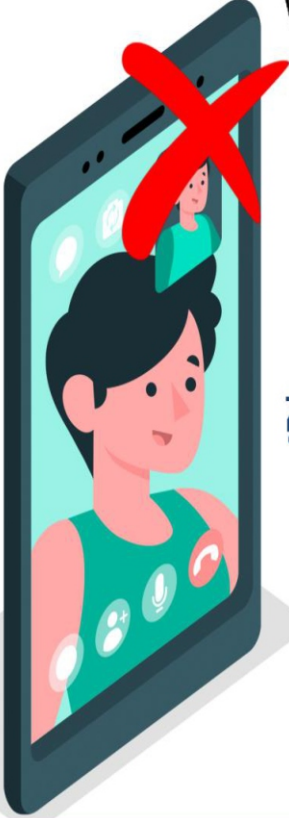
VISAKHAPATNAM CITY POLICE

www.cybercrime.gov.in



వీడియో కాల్స్ తో జాగ్రత్త

గుర్తు తెలియని వ్యక్తులతో ఎప్పుడు
వీడియో కాల్స్ మాట్లాడకండి
వేధింపులకు గురి కాకండి



సైబర్ ఫిర్యాదుల కోసం
కాల్ చేయండి **1930** కి
www.cybercrime.gov.in



విశాఖపట్నం సిటి పోలీస్

www.cybercrime.gov.in

Beware of AEPS Fraud

TO LOCK YOUR ADHAR BIOMETRIC

Download Maadhar APP from
playstore and register your
details and lock your biometric
for further stop of Aadhar
Enabled payment frauds.

Lock Your Biometric Today

Cyber Crime PS, Visakhapatnam City

call 1930 to report AEPS Fraud



#BewareOfFraudsters



FOR FURTHER SAFETY, USE BIOMETRIC LOCK/ UNLOCK FACILITY OF AADHAAR

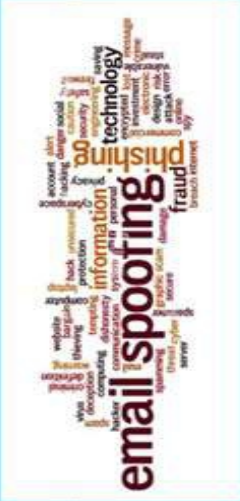
Lock/unlock your biometrics using mAadhaar App or UIDAI website.

To Lock/unlock
your biometrics
SCAN



For any assistance/query: Call **1947** (Toll-free) or email at help@uidai.gov.in

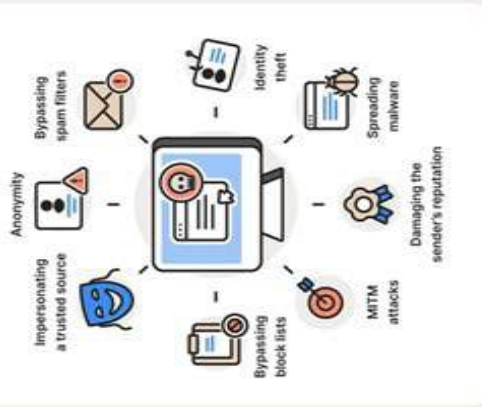




Email spoofing

In email spoofing, a cyber criminal uses a fake email address to commit a malicious act. Depending on the email spoofing tactic, they may spoof the email address, email sender's name, or both. Additionally, the cyber criminal can assume multiple identities: the sender, the company, or both.

Why Is Email Spoofing Used?



1930

CYBER CRIME POLICE, VISAKHAPATNAM CITY



Email Snooping



Snooping generally refers to the act of secretly or inappropriately looking through someone else's personal or confidential information or possessions. This could include accessing someone's private messages, emails, or browsing history without their knowledge or consent.



CYBER CRIME POLICE, VISAKHAPATNAM CITY



1930

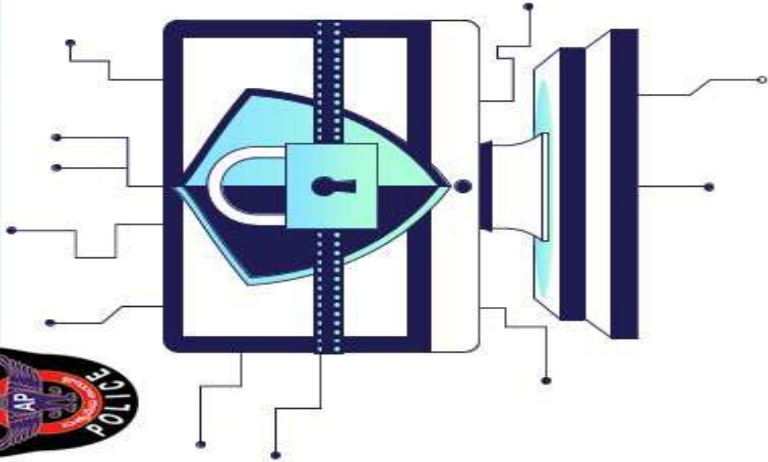


How to prevent Email Spoofing??



▲ SIGNS OF SPOOFING ▲

- 1** Sender email address is similar to the original. 
- 2** Poor grammar is used in the messages. 
- 3** The URL address does not have the "s" in the https:// 
- 4** You receive calls from unknown numbers. 
- 5** Attachments in emails seem suspicious. 



CYBER CRIME POLICE, VISAKHAPATNAM CITY

OPEN SOURCE INTELLIGENCE (OSINT) SANCHAR SAATHI PORTAL :



Sanchar Saathi portal is a citizen centric initiative of Department of Telecommunications to empower mobile subscribers, strengthen their security and increase awareness about citizen centric initiatives of the Government. Sanchar Saathi empowers citizens by allowing them to know the mobile connections issued in their name, get disconnected the connections not required by them, block/trace lost mobile phones and check genuineness of devices while buying a new/old mobile phone. Sanchar Saathi contains various modules like CEIR, TAF COP, Chakshu, etc.

CEIR:

CEIR module facilitates tracing of the lost/stolen mobile devices. This also facilitates blocking of lost/stolen mobile devices in network of all telecom operators so that lost/stolen devices cannot be used in India. If anyone tries to use the blocked mobile phone, its traceability is generated. Once mobile phone is found it may be unblocked on the portal for its normal use by the citizens.

TAF COP:

TAF COP module facilitates a mobile subscriber to check the number of mobile connections taken in his/her name. It also facilitates to report the mobile connection(s) which are either not required or not taken by the subscriber.

CHAKSHU:

Chakshu facilitates citizens to report the suspected fraud communications with the intention of defrauding telecom service users for cyber-crime, financial frauds, non-bonafide purpose like impersonation or any other misuse through Call, SMS or WhatsApp. Few examples of suspected fraud communications are communication related to Bank Account / Payment Wallet / SIM / Gas connection / Electricity connection / KYC update / expiry / deactivation, impersonation as Government official / relative, sextortion related etc.

WEB: <https://sancharsaathi.gov.in/>

నిమిషంలో మీ పోయిన ఫోన్‌ను కనిపెట్టవచ్చు



SANCHAR SAATHI

AN INTEGRATED CITIZEN CENTRIC WEB PORTAL

TRACK

- > your lost or stolen mobile device
- > your mobile connections
- > your awareness quotient

ACCESS NOW

To get mobile safety, security and assurance through features like TAFCDP, CEIR and many more...
www.sancharsaathi.gov.in



భారత ప్రభుత్వం GOVERNMENT OF INDIA
వినియోగదారుల శాఖ MINISTRY OF COMMUNICATIONS

SKIP TO MAIN CONTENT



Select Language



దूरసंचార విభాగం
DEPARTMENT OF
TELECOMMUNICATIONS



india.gov.in



HOME

ABOUT

CITIZEN CENTRIC SERVICES

KEEP YOURSELF AWARE

FAQS

IN SOCIAL MEDIA

IMAGE GALLERY

<https://www.sancharsaathi.gov.in/>

మీ పేరుపై ఎన్ని సిమ్ కార్డులు
ఉన్నాయో తెలుసుకోండి ఇలా..?

Know Number of Mobile Connections in Your Name



విశాఖపట్నం
సిటి పోలీస్

సైబర్ ఫిర్యాదుల కోసం

కాల్ చేయండి

www.cybercrime.gov.in

1930 కి

MOBILE SECURITY

Securing your mobile device from hackers involves a combination of proactive measures and ongoing vigilance. Here are some steps you can take:

Keep your device updated: Regularly update your mobile operating system, apps, and security software. These updates often include patches for known vulnerabilities.

Use strong passwords and biometric authentication: Set up strong, unique passwords for your device and all your accounts. Whenever possible, enable biometric authentication like fingerprint or facial recognition.

Be cautious of public Wi -Fi: Avoid connecting to unsecured public Wi-Fi networks, as they can be compromised by hackers. If you must use public Wi-Fi, consider using a virtual private network (VPN) to encrypt your connection.

Install security software: Use reputable antivirus and anti-malware software on your device to detect and remove threats. There are many options available for both Android and IOS devices.

Be wary of app downloads: Only download apps from official app stores like the Google Play Store or Apple App Store. Check reviews and permissions before installing any app, and avoid apps from unknown developers.

Review app permissions: Regularly review the permissions granted to each app on your device and revoke any unnecessary permissions. Limiting the access apps have to your data can help reduce the risk of unauthorized access.

Enable device encryption: Encrypting your device's data adds an extra layer of security, making it more difficult for hackers to access your information if your device is lost or stolen. Most modern smart phones have built-in encryption features that can be enabled in the settings.

Backup your data: Regularly backup your device's data to a secure location, such as cloud storage or a computer. In the event of a security breach or data loss, you'll be able to restore your information.

Enable remote wipe: Enable remote wipe functionality on your device so that if it's lost or stolen, you can remotely erase all the data to prevent unauthorized access.

Practice good browsing habits: Avoid clicking on suspicious links or downloading attachments from unknown sources, as they may contain malware. Use caution when browsing the web and be wary of phishing attempts.

By following these steps, you can help protect your mobile device from hackers and keep your personal information secure.

CYBER HYGIENE

Cyber hygiene refers to the practices and habits individuals and organizations adopt to maintain their digital security and protect against cyber threats. Here are some essential cyber hygiene methods:

Strong Passwords : Use complex passwords for all your accounts, including a mix of uppercase and lowercase letters, numbers, and special characters. Avoid using easily guessable information such as birthdays or common words.

Password Management : Utilize a password manager to generate and store unique passwords for each of your accounts. This helps you avoid using the same password across multiple accounts and makes it easier to manage your passwords securely.

Multi -Factor Authentication (MFA): Enable MFA wherever possible, especially for sensitive accounts like email, banking, and social media. MFA adds an extra layer of security by requiring multiple forms of verification to access an account.

Software Updates: Keep all your software, including operating systems, web browsers, and applications, up to date with the latest security patches. Vulnerabilities in outdated software are often exploited by cyber attackers.

Antivirus/Anti -Malware Software: Install reputable antivirus and anti-malware software on your devices and keep it updated. Regularly scan your systems for malware and other malicious software.

Secure Wi -Fi Networks: Secure your home and business Wi-Fi networks with strong passwords and encryption (WPA2 or higher). Avoid using public Wi-Fi networks for sensitive activities unless you're using a VPN.

Data Encryption: Encrypt sensitive data, both in transit and at rest, to prevent unauthorized access. Use encryption protocols such as HTTPS for web browsing and device encryption for storage.

Data Backup: Regularly backup your data to secure, off-site locations such as cloud storage or external hard drives. This ensures you can recover your data in the event of data loss or a ransomware attack.

Awareness and Training: Stay informed about the latest cyber threats and educate yourself and your employees or family members about cyber security best practices. Training programs can help users recognize phishing attempts, social engineering tactics, and other common threats.

Safe Browsing Habits: Exercise caution when clicking on links or downloading attachments in emails, messages, or social media posts, especially if they're from unknown or suspicious sources. Verify the legitimacy of websites before entering sensitive information.

Regular Audit s and Assessments: Conduct regular cyber security audits and risk assessments to identify potential vulnerabilities and areas for improvement. Address any issues promptly to strengthen your overall security posture.

By implementing these cyber hygiene methods consistently, you can reduce the risk of falling victim to cyber attacks and better protect your digital assets and personal information.

CYBER CRIME PUNISHMENT SECTIONS

The Information Technology (IT) Act, 2000 is the primary legislation in India that deals with various aspects of electronic commerce and digital communication. It was amended in 2008 and came to be known as the Information Technology (Amendment) Act, 2008. Here are some important sections of the IT Act, 2000 and its amendments:

Section 43: This section deals with penalties and compensation for damage to computer, computer systems, etc. It covers unauthorized access, downloading, copying, or introducing viruses or other malicious code into computer systems.

Section 66: It pertains to computer-related offenses such as hacking, data theft, and other cyber crimes. It prescribes punishment for those who commit computer-related crimes.

Section 66A: This section, which dealt with communication of offensive messages through electronic means, was struck down by the Supreme Court of India in 2015 for being unconstitutional.

Section 66B: It deals with punishment for dishonestly receiving stolen computer resources or communication devices.

Section 66C: This section relates to identity theft and the punishment for identity theft offenses.

Section 66D: It addresses cheating by personation by using a computer resource.

Section 66E: This section covers privacy-related offenses such as capturing, publishing, or transmitting images of private areas of individuals without their consent.

Section 66F: It pertains to cyber terrorism and the punishment for cyber terrorism-related activities.

Section 67: This section deals with the publication or transmission of obscene material in electronic form.

Section 69: It grants the government the power to intercept, monitor, or decrypt any information generated, transmitted, received, or stored in any computer resource if it is necessary for national security or in the interest of public order.

Section 70: This section deals with the protection of computer systems and data and provides for the designation of government agencies to secure these systems.

Section 79: It provides for exemptions from liability of intermediaries (such as internet service providers) in certain cases, subject to compliance with due diligence requirements.

These sections, along with others in the IT Act and its amendments, form the legal framework for addressing various cyber crimes and regulating electronic transactions and communication in India.

VISAKHAPATNAM CITY SECURITY COUNCIL (VCSC)



Visakhapatnam City Security Council (VCSC) is a not-for-profit initiative and a collaboration between Visakhapatnam City Police and Manufacturing industries, Service Industries and IT industry. Visakhapatnam city police launched VCSC, along with the Captains of Industry in Visakhapatnam to increase the preparedness pertaining to safety and security of businesses and citizens.

OUR EXECUTIVE COUNCIL



Dr. A. Ravi Shankar, IPS

Honorary Chairman



A.K. Balaji
Secretary



Lakshmi Mukkovalli
Joint Secretary (Women)



R.L. Narayana
Joint Secretary (Projects)



Dheeraj
Treasurer



Sreedhar Kosaraju
Advisor



Cyber Crime Visakhapatnam City

Are You a victim of online Financial Fraud



Dr. A. Ravi Shankar, IPS

Commissioner of Police &
Addl. District Magistrate

Visakhapatnam Metropolitan City
Andhra Pradesh

Immediately Call Helpline Number 1930

and register your complaint at
www.cybercrime.gov.in

Social Media Channels Visakhapatnam City Police



-  <https://www.youtube.com/@vizagcitypolice/>
 -  <https://www.facebook.com/visakhapatnamcitypolice/>
 -  <https://twitter.com/vizagcitypolice>
 -  <https://www.instagram.com/vizagcitypolice/>
 -  <https://whatsapp.com/channel/0029vaOHOjjHQbSDllrat1p>
- web://https://sancharsaathi.gov.in