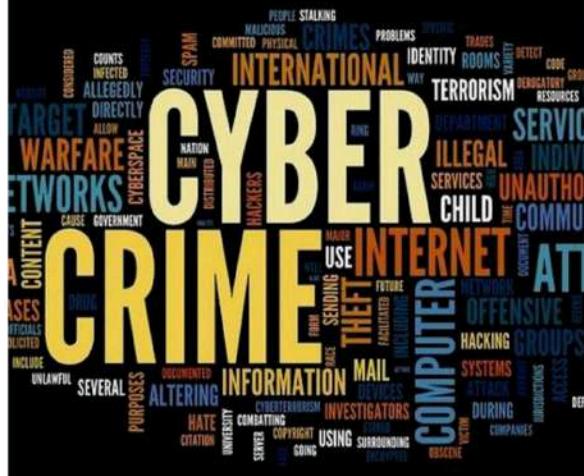




एक कदम सजगता की ओर  
सायबर अपराध निर्देशिका  
सायबर अपराध के प्रकार एवं बचने के उपाय

# Cyber Crimes

The fastest growing threat  
to service professionals



# ਵਾਟਸਅਪ ਫ਼ਾਡ

128.199.87.230 Startpage

 WhatsApp

**Congratulations!! You've been invited to try Whatsapp Calling!**

**Invite Your 10 Active Whatsapp Friends to Activate Whatsapp Calling**

- As soon as you click on "Invite Now", your whatsapp will open and you can send invitation to any of your friends
- You'll have to invite minimum 10 active friends one by one
- You can click on "Continue" after inviting 10 friends to activate voice calling on Whatsapp

**Invite Now** **Continue**

**WHATAPP  
ACCOUNT  
HACKED?**



Learning Ocean

 WhatsApp

**Your subscription is ending soon**  
Please update your payment information now.

UPDATE YOUR PAYMENT INFORMATION  
Our records indicate that your WhatsApp trial service is exceeding the one year period. At the completion of your trial period your WhatsApp will no longer be able to send or receive message. To continue using WhatsApp without interruption, we need you to subscribe for any of our subscription periods.  
**To avoid service interruption, please subscribe by visiting your account page below.**

Sign in to the customer portal with your Number:  
We appreciate your prompt attention to this matter, and look forward to continuing to meet your communication needs.

Sincerely,  
The WhatsApp Team

**Account information**  
Service: WhatsApp Subscription

## Helpful resources

[Sign in to the service portal.](#)

Have Questions? Visit the Community.

# व्हाट्सअप के उपयोग से सावधानी बरतें



- व्हाट्सअप के प्राइवेसी सेटिंग में प्रोफाईल फोटो स्टेटस आदि में “only for contacts” सेव करें।
- व्हाट्सअप में 2 स्टेप वेरीफिकेशन का प्रयोग करें।
- अपने स्वयं के नाम से जारी सिम से व्हाट्सअप का संचालन करें।
- यदि व्हाट्सअप संबंधी किसी भी प्रकार का OTP आता है तो उसे किसी के साथ शेयर ना करें।
- मोबाईल गुम या चोरी हो जाने पर तत्काल व्हाट्सअप deactivate करें।
- व्हाट्सअप वेब समय—2 पर चैक करें। कहीं कोई आपका व्हाट्सअप QR कोड स्कैन करके उपयोग तो नहीं कर रहा है।

# व्हाट्सअप का उपयोग करते समय निम्न बातों पर विशेष ध्यान रखना चाहिए –

- अनजान नम्बर से आने वाले विडियो/आडियो काल रिसीव न करें।
- अनजान व्हाट्सअप ग्रुप से न जुड़ें तथा अंजान नम्बर से आने वाले ग्रुप्स इन्विटेशन लिंक को टच ना करें।
- व्हाट्सअप में अपनी निजी/परिवारिक जानकारी शेयर नहीं करें।
- किसी भी विडियो/फोटो/मैसेज/लिंक की पुष्टि के बिना शेयर या वायरल न करें।
- सांम्प्रदायिक तथा आपत्तिजनक विडियो/फोटो/मैसेज/लिंक का प्रचार-प्रसार, पोस्ट न करें। व्हाट्सअप में आने वाले लकड़ी झा/लाटरी/ईनाम के प्रलोभन वाले मैसेज पर कोई प्रतिक्रिया न देवें।



## किसी भी फोटो/विडियो/मैसेज की सत्यता जाने बगैर फारवर्ड न करें।

- प्रत्येक ग्रुप में विभिन्न प्रकार की फोटो विडियो आते—जाते रहते हैं, उस विडियो/फोटो/मैसेज की सत्यता जांचे बिना किसी अन्य को शेयर या लाईक नहीं करना चाहिए। ऑटो डाउनलोड मोड ऑफ रखें।
- ऐसा विडियो/फोटो/मैसेज जो किसी अन्य व्यक्ति के आर्थिक, सामाजिक, राजनैतिक, स्तर को क्षति या बदनाम कर सकता है, शेयर या फॉरवर्ड न करें।
- यदि आपके द्वारा प्रेषित किसी मैसेज से किसी दूसरे व्यक्ति को क्षति कारित होती है अथवा शांति भंग होती है, ऐसी स्थिति में आप भी आपराधिक कृत्य के भागीदार बन जायेगें।



# फेसबुक

## फेसबुक उपयोग करते समय इन बातों का ध्यान रखें



- किसी अंजान व्यक्ति ग्रुप से सम्पर्क न बनाये
- पासवर्ड स्ट्रॉग रखें
- समय—समय पर पासवर्ड बदलते रहें।
- मोबाईल नम्बर/नाम/एवं जन्म तिथि को कभी भी पासवर्ड न रखें
- अन्जान व्यक्ति द्वारा भेजे गये लिंक को विलक ना करें
- प्रोफाईल फोटो को सेफगार्ड से सुरक्षित रखें
- टू फेक्टर ऑथेंटिकेशन का उपयोग करें
- यात्रा एवं खरीदी बिक्री से संबंधित जानकारी शेयर न करें
- हनीट्रैप के मामलों से बचें
- यूआर.एल का प्रयोग
- अनजान फेसबुक या सोशल मीडिया दोस्त के द्वारा झूठे गिफ्ट को प्राप्त करने के लिए अनजान व्यक्ति के बैंक खाता में पैसा जता कर देना

## अन्य सोशल साईट

- इंस्टाग्राम / ट्वीटर / हाईक / हैलो / वी-चैट / यू-ट्यूब
- जैसे सोशल साईट पर पर्सनल / प्राईवेट / कामुक / अश्लील फोटो एवं विडियो न डाले।
- फेसबुक / व्हाट्सअप की तरह ही अन्य सोशल साईट में भी सावधानी बरतनी चाहिए।
- पासवर्ड स्ट्रांग रखना चाहिए।
- अपना पासवर्ड किसी अन्य से शेयर न करें।
- किसी अन्य के मोबाईल / कम्प्यूटर / लैपटाप से सोशल मीडिया का उपयोग करने के बाद लॉग आउट / डिलीट करना सुनिश्चित करें। कोशिश करें कि अन्य के साधन का उपयोग न करना पड़े।

# गूगल

पिछले कुछ समय से हम लोग गूगल पर ज्यादा विश्वास करने लगे हैं, कुछ भी जानकारी हासिल करनी हो तो हम तुरंत गूगल साईट में जाकर सर्च कर लेते हैं तथा उस जानकारी पर विश्वास भी कर लेते हैं, इसी बात का फायदा अपराधी भी उठाते हैं। साईटों की फर्जी कॉपी कर अपना नंबर डाल देते हैं। जो गूगल सर्च इंजन में दिखता है। उन नम्बरों पर हम सम्पर्क करते हैं तो अपराधी से हमारा सम्पर्क हो जाता है और हम फ्राड के शिकार हो जाते हैं। अतः गूगल से निकाले गये फोन नम्बरों की जांच कर विश्वरस्त होने के बाद ही आगे की कार्यवाही करें, जहां तक हो सके कैश ऑन डिलीवरी से भुगतान करें।

गूगल सर्च करने पर कई तरह की फर्जी कंपनियों के वेबसाईट मिलते हैं, जो सस्ते में सामान बेचने का ऑफर करते हैं। ऐसी कम्पनी सामान की डिलीवरी के पूर्व अग्रिम भुगतान मांगती है जिन्हे कभी भी अग्रिम भुगतान न करें।

कैश रिफण्ड करने की बात कह कर भी अपराधी ठगी करते हैं। उनके द्वारा भेजे गये लिंक पर क्लिक न करें और न ही उनके झांसे में आयें। ऐसे लिंक पर क्लिक करने से आपके मोबाइल में कुछ ऐसे सॉफ्टवेयर इंस्टॉल हो जाते हैं जिनसे आपके मोबाइल का पूरा डाटा सामने वाले के पास चला जाता है।

## मैट्रिमोनियल वेबसाइट / एप

घर बैठे इंटरनेट के माध्यम से वर—वधु की तलाश विकल्प के लिए अनेक वेबसाइट एप्लीकेशन मौजूद है। जिसमें लड़का लड़की का सम्पूर्ण विवरण रहता है। जिसके आधार पर लड़का लड़की की प्रोफाईल बनाई जाती है। उक्त प्रोफाईल में लड़का लड़की को पंजीकृत होने पर एक आई.डी. नंबर दिया जाता है। और उनकी फोटो, रुचि, उम्र, परिवार, शारीरिक बनावट, शिक्षा आदि सम्पूर्ण जानकारी होती है।

# मैट्रिमोनियल वेबसाईट / एप (ध्यान रखने वाली बातें)

- बहुत ही सावधानी व सुरक्षा से वांछित साइट का चुनाव करें।
- निजी जानकारी पुष्टि उपरांत ही शेयर करें।
- लड़का लड़की का चुनाव करते समय पूर्ण रूप से जांच पड़ताल करें।
- अच्छे रिश्ते का लालच देकर पंजीयन शुल्क के नाम से वसूली की जा सकती है।
- संबंधित स्थान में अपने परिचित रिश्तेदार दोस्तों से जानकारी एकत्र करें।
- किसी भी बहाने से रुपये की मांग होने पर सावधानी बरतें।
- रिश्ते पक्का होने के नाम से अनजान लिंक/क्यूआर. कोड आदि पर भुगतान न करें।
- धोखाधड़ी होने पर तत्काल पुलिस को सूचित करें।
- रुपये मांगने वालों से रिश्ता न बनाएं।
- अति विश्वास में आकर आपत्तिजनक फोटो एंड वीडियो शेयर न करें।
- अलग-अलग मोबाइल नम्बर से फोन आने पर अकाउण्ट को डिलीट करें।
- सोशल मीडिया का उपयोग न करने वाले फर्जी हो सकते हैं क्योंकि वह अपनी पहचान छिपाते हैं।
- प्रत्यक्ष रूप से मिलने के उपरांत ही घर परिवार देखकर शादी करें।

# ऑनलाईन डेटिंग वेबसाइट / एप

## फ्राड के तरीके

- अपराधी विभिन्न सोशल साईट से फोटो तथा उसकी विस्तृत जानकारी प्राप्त कर डेटिंग एप पर फेक प्रोफाईल बनाते हैं, तथा फेक आई.डी. से फ्रेंड रिक्वेस्ट भेजते हैं।
- रिक्वेस्ट कन्फर्म होने पर चैटिंग शुरू कर लड़के लड़की को फंसाते हैं।
- अपराधी दोस्ती गहरी होने के बाद, किसी ना किसी बहाने से रुपये मांगते हैं।
- अपराधी पैसे ज्यादातर फेक नम्बर पर बनाये गये पेटीएम एकाउण्ट में लेते हैं।
- डेटिंग एप में चैटिंग के दौरान अंतरंग वीडियो, चैट, आपत्तिजनक फोटो स्क्रीन सेवर से रिकार्ड कर सोशल मीडिया में अपलोड करने की धमकी देकर रुपये की मांग करते हैं।

## ध्यान रखने वाली बातें

- जब भी आप ऑनलाईन एप डाउनलोड करे तो अपनी निजी जानकारी तुरंत साझा न करें।
- ऑनलाईन दोस्तों को निजी फोटो शेयर न करें।
- यदि आप डेटिंग एप पर चैटिंग कर रहे हैं तो भावुकता भरी बातें न करे, आप ठगी के शिकार हो सकते हैं।
- कुछ दिनों की चैटिंग के बाद रुपये की मांग या उपहार देने का लालच दे, तो सतर्क रहें।
- प्राप्त किसी अनजान लिंक को क्लिक न करें।

# ए.टी.एम कार्ड का विवरण



## ए.टी.एम. फ्राड / ए.टी.एम. क्लोनिंग

### ए.टी.एम. बूथ में होने वाले अपराध

- ए.टी.एम. कार्ड की अदला बदली कर।
- ए.टी.एम. कार्ड रीडर लगाकर।
- ए.टी.एम. कार्ड का उपयोग दूसरे को देने पर।
- ए.टी.एम. बूथ के की-बोर्ड कैंसिल बटन को खराब कर कैंसिल के जगह कंटिन्यू विकल्प से।
- ए.टी.एम. बूथ पर कैमरा लगाकर ए.टी.एम. क्लोनिंग कर।
- स्किमर का उपयोग कर।

## ए.टी.एम. बूथ (ए.टी.एम. कार्ड उपयोग करने की सावधानियां )

- ए.टी.एम. बूथ पर ए.टी.एम. कार्ड का उपयोग किसी अन्य व्यक्ति को न करने दें।
- ए.टी.एम. बूथ पर चारों तरफ ध्यान से देखें कि पोर्टेबल कैमरा/स्पाई कैमरा की—बोर्ड के ऊपर जहां से पिनकोड कवर हो रहा है उसे रिकार्ड तो नहीं कर रहा।
- ए.टी.एम. कार्ड डालने वाली जगह को ध्यान से देखें, कोई कार्ड रीडर डिवाइस या चिप तो नहीं लगा है।
- ए.टी.एम. कार्डके उपयोग करने हेतु किसी अन्य को ना भेजें।
- ए.टी.एम. कार्ड का पिन किसी से शेयर ना करें।
- ए.टी.एम. बूथ पर पिन डालते समय हाथ से कवर रखें।
- राशि निकालने के बाद कैसिंल बटन जरुर क्लिक करें।
- ए.टी.एम. से तब तक बाहर न निकले जब तक स्क्रीन का दोबारा होम पेज पर ना आ जाए।
- ए.टी.एम. बूथ पर पहले से कोई व्यक्ति मौजूद है तो पहले उसे पैसे निकालने दे, और यदि आप अंदर हैं तो कोई और उसी समय अंदर आए तो उसे बाहर भेजें।
- समय—समय पर ए.टी.एम. पिन बदलते रहें।

## ए.टी.एम. कार्ड उपयोग करने के तरीके

- संभव हो तो जिस स्थान पर सुरक्षा गार्ड हो उस ए.टी.एम. का उपयोग करें, जरुरत पड़ने पर गार्ड से सहयोग लें।
- सुनसान स्थान पर बने ए.टी.एम. से कैश निकालने से बचें।
- ए.टी.एम. बूथ में हीं कैश गिनती करें, बाहर नहीं।
- मोबाईल पर ए.टी.एम. कार्ड का पिन सेव न करें।
- अपने बैंक में मोबाईल नम्बर पंजीकृत कराये जिससे लेनदेन के सारे मैसेज प्राप्त हो।
- ए.टी.एम. के पास संदिग्ध लोग दिखे तो पुलिस को सूचित करें।
- ए.टी.एम. मशीन पर पिन डालने के बाद कैश नहीं है का मैसेज ना आए तो तत्काल बैंक को सूचित करें।

## फ्रॉड का शिकार होने पर त्वरित किये जाने वाले उपाय

- यदि आप भूलवश सायबर अपराध का शिकार हो जाते हैं तो—
- सर्वप्रथम डेबिड या क्रेडिट कार्ड को ब्लॉक करें और संबंधित बैंक एवं नजदीकी पुलिस रेस्टेशन को सूचित करें।
- मोबाइल पर आपके बैंक से आने वाले मैसेज को इग्नोर ना करें, तत्काल बैंक से सम्पर्क करें।

## शिकायत कैसे करें

निम्न जानकारी के साथ नजदीकी पुलिस स्टेशन में जाकर रिपोर्ट दर्ज कराएं –

- बैंक खाता संख्या / स्टेटमेंट की जानकारी
- ए.टी.एम. कार्ड का विवरण
- आरोपी का मोबाईल नम्बर
- मोबाईल पर आये मैसेज का स्क्रीन शॉट

## ए.टी.एम. एवं क्रेडिट कार्ड संबंधित टेलीफ्राड

अपराधी बैंक मैनेजर बन कर फोन करते हैं, और ए.टी.एम. कार्ड/क्रेडिट कार्ड ब्लॉक होने का ज्ञांसा देकर कार्ड का 16 डिजिट का नंबर एवं कार्ड के पीछे अंकित सी.वी.वी. नंबर, कार्ड वैलेडिटी डेट पूछ कर धोखाधड़ी करते हैं।

अपराधी निम्न अन्य बहाने बनाकर भी धोखाधड़ी करते हैं –

- ए.टी.एम. कार्ड/क्रेडिट कार्ड ब्लॉक होने के बहाने।
- डेबिट कार्ड/क्रेडिट कार्ड को आधार से लिंक कराने के बहाने।
- डेबिट कार्ड/क्रेडिट कार्ड की लिमिट बढ़ाने के बहाने।
- डेबिट कार्ड/क्रेडिट कार्ड के कैशबैक ऑफर के नाम पर।

ऐसा कहकर सायबर अपराधी टेलीफोन के माध्यम से आपके क्रेडिट कार्ड एवं ए.टी.एम. कार्ड तथा बैंक अकाउण्ट की जानकारी प्राप्त कर बैंक अकाउण्ट से राशि डेबिट कर लेते हैं।

## यह सायबर अपराधी निम्नलिखित जानकारी प्राप्त करता है

- डेबिट कार्ड / क्रेडिट कार्ड का 16 अंको का नंबर
- कार्ड की वैलिडिटी डेट
- कार्ड के पीछे सी.वी.वी. नंबर (3 अंको का)
- आपके मोबाईल नम्बर पर आए हुए ओटीपी
- इंटरनेट बैंकिंग का यूजर आई.डी. एवं पासवर्ड
- यू.पी.आई. आई.डी. पासवर्ड की जानकारी।

## बचने के उपाय

- बैंक कभी अपने किसी भी ग्राहक से बैंक खाते की जानकारी नहीं मांगता। अतः ऐसे कॉल आने पर प्रतिक्रिया नहीं दे।
- यदि आपके पास ऐसा कॉल आता है तो आप अपने फोन कॉल को कट कर अपने बैंक एवं नजदीकी पुलिस थाने पर संपर्क करें।
- किसी भी वास्तविक कारण के बिना किसी अन्य व्यक्ति को अपनी पहचान व जानकारी न दें।
- इन्टरनेट बैंकिंग इस्तेमाल करते समय कृपया अधिकृत बेवसाइट का ही उपयोग करें। (<https://>) एवं URL के साइड में ताले का चिन्ह वाली साइट पर ही जाए।
- अनजान ईमेल / एस.एम.एस से प्राप्त लिंक पर क्लिक न करें।
- इंटरनेट बैंकिंग इस्तेमाल करने के लिए फ्री वाईफाई या पब्लिक इंटरनेट का इस्तेमाल करते समय सावधानी बरतें।

# ओ.एल.एक्स / विवकर फ्राड से बचने के उपाय

- कोई भी वाहन/मोबाईल/अन्य सामान को खरीदते एवं बेचते समय सावधानी बरते।
- वाहन/मोबाईल/अन्य सामान पसंद आने पर तत्काल भुगतान न करें। एडवांस रकम के नाम पर आपसे धोखाधड़ी हो सकती है।
- ओ.एल.एक्स / विवकर आदि पर पुलिस/आर्मी/अर्धसैनिक बल के सुरक्षाकर्मी के पहचान पत्र के नाम पर ठगी की जा रही है तत्काल विश्वास न करें।
- पुलिस/आर्मी/अर्धसैनिक बल के पहचान का भी दुरुपयोग ठग के द्वारा किया जा रहा है। अतः उनके पहचान/नंबर का भी जांच पड़ताल करने के उपरांत ही खरीदी/बिक्री करें। विडियो कॉल/प्रत्यक्ष रूप से देखकर सामान की खरीद करें।
- ओ.एल.एक्स/विवकर आदि पर खरीदी/बिक्री हेतु पोस्ट की गई वाहन/मोबाईल/अन्य सामान की केवल फोटो को देखकर सौदा न करें, सामान को जांच परख कर ही लेनदेन करें।
- ओ.एल.एक्स / विवकर पर वाहन बेचते/खरीदते समय किसी लेन-देन भुगतान हेतु किसी लिंक पर विलक, ऑनलाईन पेमेंट न करें। (01 रु., 10 रु के भुगतान के नाम पर लिंक/क्यूआर. कोड भेजकर आप के साथ ठगी हो सकती है)
- ऑनलाईन सामान खरीदते समय कैश ऑन डिलीवरी विकल्प का ही उपयोग करें।
- कम कीमत, आकर्षक मूल्य के झांसे में ना आयें।



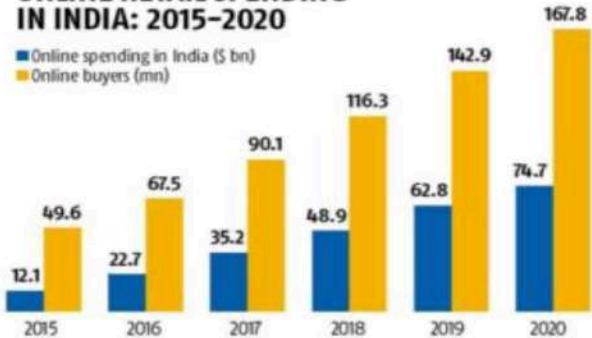
# ई-कामर्स साईट

Top 5 E-Commerce Websites in India



## ONLINE RETAIL SPENDING IN INDIA: 2015-2020

■ Online spending in India (\$ bn)  
■ Online buyers (mn)



Source: Forrester research online retail forecast, 2015-2020, Asia-Pacific

## India's e-commerce potential

Online buyers  
(in million)

100\*  
2017



\*expected to cross

Industry size (in \$ billion)



\*\*expected to reach

Population

1.4bn

by 2020, half of  
it middle-class

## Online spending by value

Apparel (85%)   Mobile phones (68%)   Cosmetics (25%)

## Internet users

600mn  
Expected to reach by 2020

Source: Assocham-Resurgent India study, EY

## ई-कामर्स साईट

इंटरनेट के माध्यम से व्यापार का संचालन, खरीदी बिक्री हेतु ग्राहकों के लिए सेवाएं उपलब्ध कराना ही ई-कामर्स है।

### ई-कामर्स साईट में अपराध के तरीके

- अपराधी ऑनलाईन खरीदी/बिक्री या सेवा देने वाली विभिन्न कंपनी के साईट्स को कॉपी कर फर्जी साईट बनाकर फर्जी नंबर डिस्प्ले करते हैं। लोग इन फर्जी साईट पर जाकर ऑनलाईन सामान आर्डर कर पैसे का अग्रिम भुगतान करते हैं और ठगी का शिकार हो जाते हैं। सही साईट्स का चयन करे तथा फर्जी साईट्स से बचे।
- अपराधी कहते हैं कि आप हमारे लकड़ी कस्टमर है आपका मोबाईल नंबर लकड़ी ड्रा में निकला है, आपने कार/कोई मंहगी वस्तु/नगद राशि जीती है कहकर धोखाधड़ी करते हैं।
- ऑनलाईन पेमेंट न करें। (01 रु., 10 रु के भुगतान के नाम पर लिंक/क्यूआर. कोड भेजकर आप के साथ ठगी हो सकती है)

## ई-कामर्स साईट में अपराध के तरीके

- लकड़ी ड्रा से जीती हुई कार/मोटर साईकिल/अन्य सामान के रजिस्ट्रेशन/ट्रांसपोर्टेशन/इंश्योरेंस/सर्विस शुल्क/जी.एस.टी.आदि का झांसा देकर फर्जी खाते में पैसा जमा करा लेते हैं।
- अपराधी नगद राशि भेजने के नाम पर बैंक/ए.टी.एम. संबंधित सभी प्रकार की जानकारी एवं ओ.टी.पी. प्राप्त कर खाता से पैसे आहरण कर लेते हैं।
- किसी प्रकार के ईनाम/लकड़ी ड्रा/प्रलोभन/आकर्षक स्कीमके झांसे में न आवें।
- ई कामर्स साईट पर वाहन/अन्य सामान क्रय विक्रय करते समय किसी रकम का भुगतान हेतु किसी लिंक पर क्लिक, आनलाईन पेमेंट न करें।(01 रु., 10 रु के भुगतान के नाम पर लिंक/क्यू.आर. कोड भेजकर आप के साथ ठगी हो सकती है)

# ऑनलाईन शोपिंग फ्राड



**Fraud Site - No More Exist**

**A R shopee**  
Affordable Rates Shopping

shopping on the go  
Fast & Easy

× × × × ×

## ऑनलाईन शोपिंग करते समय निम्न सावधानियां बरतने की जरूरत है

- अनजान व्यक्ति /अनजान वेबसाइट पर अपने बैंक एकाउण्ट डेबिट/क्रेडिट कार्ड से संबंधित जानकारी साझा न करें।
- कम्प्यूटर या मोबाईल पर आपरेटिंग सिस्टम/एंटी वायरस को समय—समय पर अपडेट करते रहें।
- किसी ऑनलाइन पोर्टल में खरीददारी करने से पहले यह सुनिश्चित कर लें कि सही वेबसाइट/एप का उपयोग कर रहे हैं।
- https & http – जिस वेबसाइट से सामान खरीद रहे हैं, उसके एड्रेस (यू.आर.एल) में https होना चाहिए, ना कि http क्योंकि s का मतलब सिक्यूरिटी की गारंटी से है।
- ऐसे वेबासाईट या एप से खरीददारी करें जिसमें ऑफिस का पता ई मेल व हेल्प लाईन का नंबर सही व स्पष्ट हो।

## ऑनलाईन शॉपिंग करते समय निम्न सावधानियां बरतने की जरुरत है

- गलत वेबसाईट लालच/आकर्षक/लुभावने आफर करते हैं और हमारी जानकारी चुराने का माध्यम बन जाते हैं।
- ऑनलाईन शॉपिंग करने के बाद निश्चित हो जाना महंगा पड़ सकता है। बैंक स्टेटमेंट का समय समय पर जांच करते रहना चाहिए।
- ऑनलाईन शॉपिंग के कुछ समय/दिन बाद यदि उसकी शॉपिंग का हवाला देकर यदि कोई अनजान फोन कर्ता लुभावनी बात करता है तो उसके झांसे में न आयें।
- सामान प्राप्त करने के बाद उसे डिलीवरी बॉय के सामने ही चेक करें गडबडी होने पर डिलीवरी बॉय के साथ/सामने ही फोटो खींच लें।
- केश ऑन डिलीवरी पेमेंट मोड का इस्तेमाल करें।

# लिंक फ्राड

सायबर अपराधी के द्वारा विभिन्न एप एवं टूल्स से तैयार लिंक लोगों के पास भेजे जाते हैं उसे विलक कर देने से हमारे मोबाइल में उपलब्ध बैंक संबंधी गोपनीय जानकारी जैसे ओ.टी.पी., पिन नम्बर आदि अपराधी के पास चले जाते हैं। अतः ऐसे अवांछित लिंक को विलक करने से बचना चाहिए।

**From:** support@ucdavis.edu [mailto:support@ucdavis.edu]

**Sent:** Sunday, June 16, 2013 11:06 AM

**To:** support@ucdavis.edu

**Subject:** Account at Risk

Your Email account is at Risk, follow the link below and sign on to resolve this error.

hold your mouse over the link to see where the link  
is actually directing you - you should see the  
link/redirect address

<https://cas.ucdavis.edu/login.html>

Failure to do so would lead

[http://commercialcleaning.kiwi.nz/image/  
data/davis.htm](http://commercialcleaning.kiwi.nz/image/data/davis.htm)

Ucdavis Support

suspicious link address



Text Message  
Today, 11:32 AM

Your K.Y.C has been updated  
successfully, you will get 1205  
cashback in your wallet, To get  
cashback click here Link  
<http://8629a7f1.ngrok.io>

## लिंक फ्राड कैसे होता है

- ठग फोन से बात कर ज्ञांसा देकर लिंक भेजते हैं जिस पर हम लिंक विलक कर प्रतिक्रिया देते हैं।
- मेल/पोस्ट/मैसेज के माध्यम से लिंक भेजकर।
- 01 रु या 10 रु के भुगतान व सत्यापन/पंजीयन के बहाने।
- आकर्षक ईनाम/लाटरी/ लकड़ी ढांचे के नाम से लिंक भेज कर।
- सोशल मीडिया से लिंक भेजकर।

## बचने के उपाय

- अनजान कोई भी लिंक को विलक न करें।
- मोबाईल पर आकर्षक ईनाम/लाटरी/लकड़ी ढांचे के नाम पर भेजे गये लिंक को विलक न करें।
- सोशल मीडिया से भेजे गये अंजान लिंक पर विलक न करें।
- कभी भी आपको कोई ऐसा लिंक दिखे जो आपको अमीर बनाने का वादा करता हो, उस लिंक को विलक न करें।
- पेंशन/ईश्योरेंस/मैच्युरिटी के नाम पर भेजे

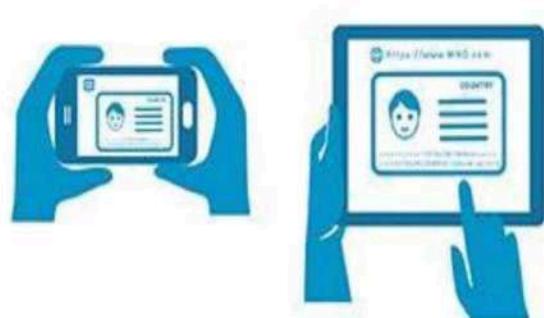
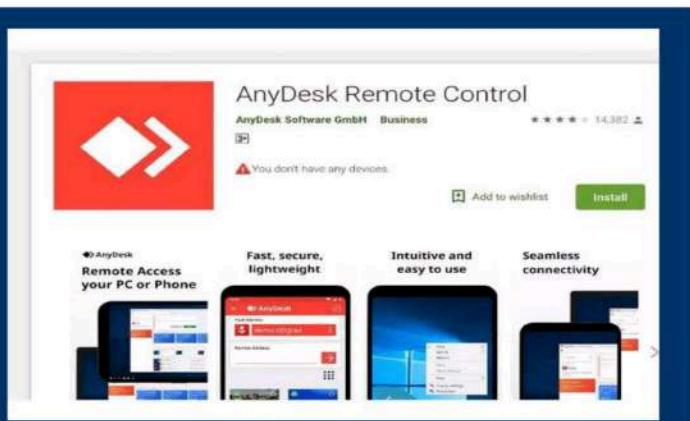
## लिंक फ्राड

ध्यान मे रखने योग्य बातें :-

- फोन पर बैंक / एटीएम / ओटीपी की जानकारी न देवे।
- रजिस्ट्रेशन / सर्विस / एडवांस / कमीशन के नाम पर कोई भुगतान न करे।
- लोन के नाम से आये अनजान मेल / मैसेज / काल पर कोई प्रतिक्रिया न दें।
- लोन के नाम से 1 रुपये / 10 रुपये का भुगतान, अनजान लिंक पर विलक न करें।
- लोन के नाम से अनजान व्यक्ति को अपनी व्यक्तिगत जानकारी एवं दस्तावेज न दें।
- कोशिश करें कि बैंक जाकर ही लोन के लिये आवेदन करे और दस्तावेज दें।

# अवांछित एप डाउनलोड करना

साइबर क्रिमिनल द्वारा लोगों को ज्ञांसा देकर रिमोट एप्लीकेशन जैसे टीम विवर, एनी-डेस्क, एयरड्रायड, क्रोम रिमोट डेस्कटॉप जैसे एप्लीकेशन डाउनलोड करा देते हैं जो हमारे मोबाईल को रिमोट के माध्यम से आरोपी अपने मोबाईल में पैरेलल (सीधे) देख सकते हैं और इसी एप्लीकेशन के जरिये हमारे ओ.टी.पी. पिन नंबर एवं अन्य बैंक संबंधी गोपनीय जानकारी प्राप्त कर धोखाधड़ी करते हैं, अतः अनजान एप्लीकेश को अपने मोबाईल में बिल्कुल भी डाउनलोड/इंस्टाल न करें।



## लोन फ्राड



लोन देने के बहाने भी बहुत सारे किमिनल हमें फोन कर तरह—तरह की लुभावने स्कीम का झांसा देकर पहले डाक्यूमेंटेशन फीस के रूप में 2000—3000 रु० जमा करवाते हैं, हम अत्यधिक रकम नहीं होने से आसानी से उनके बताये खाते में रकम जमा करा देते हैं, धीरे—धीरे आरोपी रकम बढ़ाते जाते हैं और एक बड़ा रकम जमा करा कर हमसे धोधाखड़ी करते हैं। ऐसे कॉल एवं लोन देने वाले लोगों से हमें बचना चाहिए तथा लोन देने के लिए बने हुए वैध संस्थानों से ही लोन लेना चाहिए, अन्य के झांसे में नहीं आना चाहिए।

## लॉटरी फ्राड



आये दिन हमारे मोबाईल फोन पर लाटरी लगने, कैश बैंक मिलने या अन्य आफर संबंधी मैसेज आते रहते हैं जो सायबर अपराधियों द्वारा फैलाया गया जाल होता है। यदि हम इनके झांसे में आ जाते हैं तो वे लाटरी लगने का लालच देकर डाक्यूमेंटेशन चार्ज, जी.एस.टी.चार्ज, ट्रांसपोर्टेशन चार्ज रजिस्ट्रेशन के नाम से काफी बड़ी रकम अपने खाते में जमा करवा लेते हैं या धोखे से हमसे ओटीपी या पिन प्राप्त कर हमारे बैंक खातों में जमा राशि निकाल सकते हैं।

# लॉटरी फ्राड



## धोखाधड़ी का तरीका एवं बचाव संबंधी उपाय

- सायबर अपराधी इंडियन गवर्मेन्ट/डिजीटल भारत/प्रधानमंत्री/मुख्यमंत्री की फोटो का उपयोग कर भी ठगी करते हैं किसी भी लालच में आकर अनजान खाते में पैसा जमा न करें।
- व्हाट्सअप पर लोगों के पास अंजान नंबरों से काल आता है तथा व्हाट्सअप की तरफ से आपकी लॉटरी लगी है कहते हुए जीती हुई रकम प्राप्त करने के लिए मुबई अथवा दिल्ली के किसी अन्य का नंबर देकर उसे मैनेजर बताते हैं और वह प्रोसेसिंग फीस (के.वाई.सी) अपडेट आदि नाम से भिन्न भिन्न फर्जी खातों में पैसा जमा कराते हैं। इससे बचे।
- कौन बनेगा करोडपति के नाम से कॉल या मैसेज कर/हिस्सा लेने के नाम से बैंक खातों में पैसा जमा कराते हैं ऐसे ठग अपराधियों के झांसे में न आयें।
- लॉटरी/गिफ्ट या किसी अन्य चीज के लिए एकाउण्ट वेरिफिकेशन के नाम पर ओटीपी शेयर न करें।
- अनजान सोर्स से आये लुभावने स्कीम के यूआर.एल. लिंक पर क्लिक न करें।

# बीमा / पेंशन / ई.एम.आई फ्राड



साइबर अपराधियों द्वारा हमारे इंश्योरेंश / पेंशन / ई.एम.आई. / मोबाईल नंबर से संबंधित जानकारी प्राप्त लोगों को फोन कर पर्सनल डिटेल जैसे पॉलिसी नंबर, नाम, बीमा की रकम, मैच्युरिटी दिनांक आदि बताते हैं, जिससे हम उनकी बातों में आकर कमीशन बचाने, अधिक लाभ प्राप्त करने के लालच में आकर तथा पॉलिसी लैप्स होने से बचाने के लिए आरोपियों के बताए अनुसार आरोपी के खाते में पैसा जमा कर देते हैं और उग्री के शिकार हो जाते हैं।

यदि अनजान काल आये तो आप सबसे पहले अपने नजदीकी बीमा कंपनी जाकर मिले तथा फोन काल के सम्बन्ध में जानकारी देवें। पुलिस एवं सायबर सैल से अविलंब सम्पर्क करें।

## टॉवर फ्राड



- मकान/जमीन पर टॉवर लगाने तथा बहुत अधिक रकम किराये के रूप में देने का लालच देकर क्रिमिनल धोखाधड़ी करते हैं।
- फोन या अखबार में यदि इस प्रकार से टॉवर लगाने संबंधी फोन कॉल आये या विज्ञापन दिखे तो अच्छी तरह से इसकी सत्यता की जांच संबंधित फोन कम्पनी/पुलिस/सायबर सैल से करा कर ही पैसा खर्च करें अन्यथा फ्राड का शिकार हो सकते हैं।

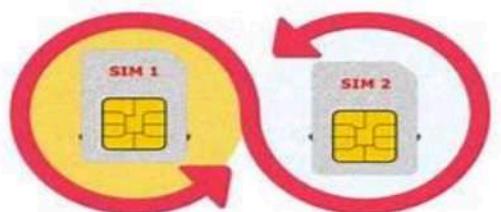


- मोबाईल कंपनी को यदि टावर लगाना होता है तो आवश्यकतानुसार क्षेत्र का भ्रमण/सर्वे कर स्वयं जमीन/प्लाट/मकान की खोज करते हैं। किसी भी खाली जमीन/प्लाट/मकान पर कंपनी टावर नहीं लगाती है।
- कोई भी कंपनी टॉवर लगाने से पहले किसी भी प्रकार के रकम की मांग नहीं करती है। अतः किसी के घोखे में न आयें।
- टावर के नाम से एडवांस/कमीशन के नाम पर भुगतान न करें।

# सिम स्वैपिंग / सिम फ्राड

आपके द्वारा उपयोग की जा रही सिम (मोबाइल नम्बर) जिस भी कंपनी का है उसे बंद करवा कर अपराधी अपने पास रखें खाली/ब्लैंक सिम में परिवर्तित चालू कर आपके नंबर का गलत उपयोग करने लगते हैं।

## How To Prevent



## SIM Swap Fraud Attack

INFOLEADING.COM





1. The fraudster steals the bank customer's credentials and mobile number



2. The fraudster manipulates the mobile operator to perform a SIM swap on the customer's mobile number



5. The OTP arrives on the fraudster's mobile device and is used to access the customer's account

## SIM-SWAP FRAUD



4. The bank sends an SMS OTP to the customer's mobile number



3. The fraudster uses the customer's credentials to initiate a login to their online banking account

## कैसे होता है सिम स्वैपिंग

- अपराधी फर्जी नंबर से नेटवर्क सुधारने/इंटरनेट की स्पीड बढ़ाने के लिए कॉल करते हैं। 3जी से 4जी या 5जी अपडेट करने तथा लाटरी/ईनाम आदि का बहाना बनाकर सिम के पीछे प्रिंट 20 अंको के आईसीसीआईडी कोड पूछ लेते हैं।
- सिम के पीछे सिम नम्बर 20 अंको का बताते ही अपराधी हमे 01 प्रेस करने को कहता है। 01 प्रेस करना हमारी सिम स्वैपिंग की स्वीकृति होती है।
- 20 अंको को बताने के बाद 01 ओटीपी मैसेज के रूप में आता है, जिसे बताते ही सिम स्वैपिंग हो जाता है।

## बचने के उपाय

- किसी भी व्यक्ति को सिम के पीछे लिखे 20 अंको का नंबर नहीं बताना चाहिए।
- अगर आपका सिम कुछ घंटों के लिए अचानक बंद हो जाता है तो तुरंत अपने ऑपरेटर से संपर्क करें।
- जिस सिम (मोबाइल नम्बर) से आपका बैंक खाता लिंक है उसे सोशल मीडिया पर डिस्प्ले न करें।
- ओ.टी.पी. अन्जान व्यक्ति को कभी ना बताएं।

## जॉब फ्राड

वर्तमान समय में लोग घर बैठे ही नौकरी हेतु आवेदन कर रहे हैं, समाचार पत्र के विज्ञापन, मैसेज, मेल व कॉल पर प्रतिक्रिया दे कर व पैसे देकर धौखाधड़ी के शिकार बन जाते हैं।



## जॉब फ्राड के तरीके

- लुभावनी / अधिक / आकर्षक सैलरी का प्रलोभन।
- अनजान ई—मेल / मैसेज / कॉल द्वारा।
- फर्जी कंपनी के नाम से फर्जी कॉल सेंटर द्वारा कॉल कर।
- फर्जी वेबसाइट द्वारा।
- जॉब के आवेदन व जॉब में लगने के लिए रूपये की मांग करना।
- अधिकतर जॉब ऑफर से सम्बन्धित फर्जी मेल उन कंपनी के नाम से आते हैं जिनके बारे में आप काफी अच्छे से जानते हैं।
- नौकरी के नाम से आवेदन / पंजीयन शुल्क एडवांस भुगतान के नाम पर।
- जॉब रिप्लेशमेंट / काल सेंटर के द्वारा वांछित कंपनी की जानकारी देने के एवज में ठगी।
- एडवांस ट्रेनिंग शुल्क के नाम से ठगी।

## जॉब फ्राड पर ध्यान रखने योग्य बातें

- अधिकृत वेबसाइट/विभाग का ही चयन करें।
- नौकरी के संबंध में पूर्ण जांच पड़ताल करें।
- विज्ञापन पर जॉब के नाम से अपनी निजी जानकारी/दस्तावेज शेयर करते समय सावधानी बरतें।
- फर्जी सरकारी नौकरी के ऑफर को पहचानें।
- नौकरी से संबंधित अनचाहे ई-मेल पर कोई जवाब न दें।
- वेबसाइट पर दिखने वाले नौकरी से संबंधित विज्ञापनों से बचें।
- असली और नकली वेबसाइट की पहचान करना सीखें।
- ऑनलाइन इंटरव्यू पर सावधानी बरतें।
- जॉब पोर्टल यानी नौकरी खोजने वाली वेबसाइट में पंजीकरण से पहले प्राइवेसी पॉलिसी अवश्य देखें।
- नौकरी के सम्बन्ध में अपने माता पिता या संरक्षक को अवश्य बतायें।
- यदि कोई वेबसाइट नौकरी दिलवाने का दावा करती है तो उस दावे से संबंधित खोजबीन अवश्य करें।
- यदि कोई व्यक्ति किसी कंपनी में जॉब दिलवाने का दावा करता है तो उस कंपनी में पूछताछ करें व उससे उसके उस कंपनी में होने का साक्ष्य मांगें।
- समाचार पत्रों/गूगल डिस्प्ले पर आये विज्ञापन व प्राप्त मैसेज/मेल/कॉल पर रकम का भुगतान न करें।

## फ्राड के तरीके

- ऐसे साइट में संपर्क करने पर पूरी डिटेल्स जैसे आधार कार्ड, फोन नम्बर, बैंक डिटेल्स, फोटो आदि ले लिया जाता है।
- हस्ताक्षर लेकर धोखे से एग्रीमेंट पर साइन करा लेते हैं।
- 7 दिन में काम पूरा करने के लिए बोला जाता है।
- बात ऐसे किया जाता है कि आप इस वर्ग को 7 दिन में पूरा करके दिखाओ उसके बाद आप को परमानेंट हमारे कंपनी में जॉब दिया जायेगा।
- यदि आप काम छोड़ते हैं तो जालसाज द्वारा आप को फोन पर धमकी देते हैं आपके ई-मेल पर एग्रीमेंट के नाम पर कोर्ट का फर्जी नोटिस भेजते हैं।

## बचने के उपाय

- विश्वासपात्र साइट पर ही विजिट करें।
- कोई भी फ्रीलांसर जॉब साइट एग्रीमेंट के नाम पर पैसा नहीं मांगता।
- आपके ई-मेल पर आए फर्जी कोर्ट के नोटिस से न डरें।
- ऐसे जालसाजी के शिकार होने पर अपने नजदीकी पुलिस स्टेशन जाकर शिकायत करें।

## फर्जी सरकारी नौकरी के ऑफर को पहचाने

- जाली व नकली वेबसाईट की पहचान करने का तरीका उनकी वेबसाईट की स्पेलिंग में अंतर होना, गलत लिखी होना आदि।
- सरकारी विभाग से सम्बन्धित उनकी अधिकृत वेबसाईट में .gov.in और सरकारी विभाग से सम्बन्धित नौकरी के विज्ञापन समाचार पत्र में या रोजगार समाचार पत्र में प्रकाशित होते हैं।