साइबर क्राइम सेल गोण्डा
जागरूकता अभियान

जागरुक रहे। सावधानी ही बचाव हैं। सुरक्षित रहें।

साइबर अपराधियों द्वारा आमजन को निम्नलिखित माध्यम से धोखाधड़ी का शिकार बनाया जा रहा है।

➢ सिम कार्ड फ्रॉड - अनजान नम्बर से काल आने पर आपको सावधान रहने की जरूरत है। अपराधी आजकल सिम स्वैप कर बैंक खाते से पैसा निकाल ले रहे, जिसमें कॉल करके कस्टमर को बताया जाता है कि ये कॉल कस्टमर केयर की तरफ से हैं, नेटवर्क प्रॉब्लम है जिसे अपडेट करने के लिए यूजर से कोई बटन (नंबर की दबाने को कहा जाता है और आपका सिम स्वैप हो जाता है। ऐसे कॉल से बचें। किसी भी प्रकार की समस्या होने पर सीधे कस्टमर केयर के नम्बर पर ही सम्पर्क करें।

➢ एटीएम कार्ड फ्रॉड - अपना एटीएम कार्ड किसी भी अन्य व्यक्ति को कदापि न दे और न ही किसी से सहायता ले। एटीएम बूथ के अन्दर पैसा निकालते समय पिन हमेशा अपनी हथेली से छिपाकर डालें। जब भो पैसा निकालने जाये किसी अन्जान व्यक्ति को बूथ के अन्दर न प्रवेश करने दे। एटीएम वहाँ प्रयोग करे जहाँ गार्ड मौजूद हो।

➢ डेविट / क्रेडिट कार्ड स्वाइप फ्रॉड - कार्ड स्वैप मशीन का प्रयोग स्वयं करें। किसी अन्य व्यक्ति को स्वैप करने के लिए न दे। शापिंग मॉल, होटल, पेट्रोल पम्प पर इस्तेमाल करते समय हिडन कैमरा का ध्यान विशेष ध्यान रखें। स्वैप मशीन के अलावा किसी अन्य डिवाइस पर कार्ड स्वैप न करें।

➢ बायोमैटिक फ्रॉड साइबर - अपराधी आपके अंगठे का क्लोन बनाकर के पैसा निकाल ले रहे है। किसी भी अनजान व्यक्ति को अपना अंगूठा किसी भी फार्म पर लगाकर मत दें। ग्राहक सेवा केन्द्र पर आधार पेमेन्ट के माध्यम से पैसा निकालते समय अपने अंगूठे का इस्तेमाल सावधानी पूर्वक करें। आधार कार्ड, पैन कार्ड, राशन कार्ड, नयी सिम लेने के लिए कई बार फिंगर स्कैन न करें।

➢ यू०पी०आई० फ्रॉड - मोबाईल फोन पर अज्ञात यूपीआई लिंक कदापि ओपन न करें। किसी के कहने पर कोई भी लिंक या मैसेज किसी अन्य मोबाईल नम्बर पर फारवर्ड न करे। अपना यूपीआई पिन किसी अनजान यूपीआई लिंक पर न डाले। यूपीआई(गूगल पे. फोन-पे या पेटीएम) पिन का प्रयोग करने से एवं QR कोड स्कैन करने से पैसे आपके ही खाते से कटते हैं। किसी से पैसा लेने के लिए कभी पिन की आवश्यकता नहीं होती। किसी फोन कॉल पर किसी के कहने से अपना पिन डालकर बैलेंस न चेक करें। कस्टमर केयर नं० गूगल से सर्च न करें।

➢ फोन कॉल बैंकिंग फ्रॉड - आपका बैंक खाता/एटीएम बन्द हो गया है या आपका नंबर पुनः रजिस्टर कराने हेतु, क्या आप इसे चालू रखना चाहते हैं, इस तरह के फोन कॉल से बचे। बोनस प्वाइंट, रिवार्ड प्वाइंट, कैशबैक, KBC आदि लुभावने ऑफर के लालच में अपने बैंक डिटेल फोन पर शेयर न करें। अपने फोन पर आये ओ०टी०पी० को किसी से साझा न करें। किसी प्रकार का सपोर्ट एप्स जैसे टीमविवर, ऐनी डेक्स आदि किसी के कहने पर मोबाइल में इनस्टॉल न करें।

➢ <u>पालिसी, चिट फण्ड, लॉटरी एवं जॉब सम्बन्धित फ्रॉड -</u>फोन/ समाचार पत्र, पत्रिका में दिये विज्ञापन का सत्यापन करने के पश्चात ही आवेदन करें। ऐसे जॉब आफर लिंक जिसके लिए आवेदन नहीं किया है उसको ओपन न करें। लाटरी, जॉब प्राप्त करने जैसे लुभावने स्कीम के लालच में न आये। कम समय में पैसा डबल करने जैसे लुभावने स्कीम के लालच में न आये।

➢ <u>लोन एप फ्रॉड-</u> सस्ते एवं आसान लोन के लालच में प्ले स्टोर से कोई भी लोन एप डाउन न करें, क्योकि ये एप आसानी से लोन देकर आपके फ़ोन का निजी डेटा(Contact, gallery) ले कर आपको अत्यधिक ब्याज चुकाने के लिए आपके रिश्तदारों एवं मित्रों को परेशान करते है। लोन हमेशा अधिकृत बैंक से ही ले। अनाधिकृत लोन एप से बचें।

➢ <u>OLX समान खरीदने व बेचने से सम्बन्धित फ्रॉड -</u> कोई व्यक्ति आपके सामान को खरीदने के लिए ऑनलाईन पेमेंट करने को बोले तो पेमेंट करने से बचे। सेना के जवान बनकर सामान बेचने वाले व्यक्ति का वेरीफिकेसन जरुर करें, डिलीवरी मिलने से पहले कोई भी पेमेंट न करे। सस्ते के लालच में किसी खाते में एडवांस पेमेंट न करें।

➢ <u>सोशल मीडिया सम्बन्धित फ्रॉड -</u> सोशल नेटवर्किंग साइट पर अपनी व्यक्तिगत सूचनाओं को कम से कम साझा करें। अपना पासवर्ड किसी भी व्यक्ति से शेयर कदापि न करें। सभी सोशल मीडिया प्लेटफार्म पर 2 स्टेप वेरिफिकेशन आन रखें। अपने मोबाइल नंबर, मेल एवं मित्रों की सूची छिपा कर रखें। प्रोफाइल लॉक रखें। किसी अन्य मोबाईल या डेस्कटाप पर अपनी सोशल मीडिया आईडी ओपन करने से बचें, सोशल मीडिया पर किसी भी आपत्तिजनक भड़काउ झूठी सूचनाओं को पोस्ट, लाईक, कमेन्ट, शेयर करने से बचे। अनजान लोगो का फ्रेन्ड रिक्वेस्ट स्वीकार करने से बचे। अनजान महिला से चैट न करें न ही अपना whatsapp नंबर शेयर करें।

➢ <u>WhatsApp से सम्बन्धित फ्रॉड-</u> WhatsApp पर अज्ञात महिला/व्यक्ति का वीडियो कॉल कतई स्वीकार न करें। यदि आप का अश्लील वीडियो किसी ने बना लिया है एवं आपसे सम्बन्धित लोगों को इस वीडियो को वायरल करने की धमकी देकर पैसे की माँग की जाती है तो बिना घबराये उस नंबर को ब्लाक करें एवं किसी धमकी से डर कर पैसे नही दें। किसी भी व्यक्ति को अपने व्हाट्सप का बारकोड स्कैन करने न दे और न ही किसी अनजान व्यक्ति का भेजा हुआ बारकोड स्कैन करें। व्हाट्सप पर किसी अनजान व्यक्ति द्वारा भेजे गए लिंक को न खोले। लिंक के कारण आप धोखाधड़ी के शिकार हो सकते हैं। । व्हाट्सप में हमेशा 2 स्टेप वेरिफिकेशन आन रखें।

➢ वित्तीय साइबर अपराध का शिकार होने पर तत्काल साइबर हेल्प लाइन नम्बर 1930 या 112 पर दे एवं नजदीकी पुलिस स्टेशन में साइबर हेल्प डेस्क पर रिपोर्ट करें, अन्य साइबर अपराध की रिपोर्ट वेबसाइट https://cybercrime.gov.in/ पर अथवा UPCOP एप के माध्यम से भी की जा सकती है।

(लक्ष्मीकान्त गौतम) PPS	(शिवराज) PPS	(आकाश तोमर) IPS
क्षेत्राधिकारी क्राइम	अपर पुलिस अधीक्षक	पुलिस अधीक्षक
गोण्डा।	गोण्डा।	गोण्डा।