सायबर फसवणुक वेगवेगळया पध्दतीने होत आहे. त्यामध्ये सध्या पिंपरी-चिंचवड आयुक्तालयातील बरेचशे लोक लोन ॲप ट्रॅपमध्ये फसलेले आहेत. या प्रकारामुळे बरेचशा लोकांनी नैराश्यातुन आत्महत्या करण्याचा प्रयत्न केला आहे. या प्रकाराला घाबरुन न जाता त्याला सामोरे कसे जायचे हे समजुन घ्या.

Instant Loan App पासुन सावधान....

➢ गुन्हा करण्याची पध्दत –

- **Instant Loan** घेण्यासाठी आपल्याला **SMS, Whats App** मेसेज करुन घरबसल्या लोन घेण्याचे आमिष दाखविले जाते.
- **Instant Loan App** डाऊनलोड करण्यास सांगितले जाते. त्यासाठी **link** किंवा **Play store** वरुन ॲप डाऊनलोड करण्यास सांगितले जाते.
- तुमचे आधारकार्ड, पॅनकार्ड, बँक डिटेल्सचे कॉपी अपलोड करण्यास सांगितले जातात.
- **Loan App** डॉउनलोड केले की तुमचे सर्व **Contact Number, Photo, Internal Memory** चा **Access** घेतला जातो.
- तुमच्या ॲप मध्ये लोन क्रेडिट झाल्याचे दाखवले जाते.
- दोन तीन दिवसातच लोन पूर्ण भरण्यास सांगतात नाहीतर दुप्पट रक्कम भरावी लागण्याची धमकी देतात. व्याजदर हा अवास्तव असतो.
- तुम्ही लोन पुर्ण भरले तरीही तुमच्याकडे पैश्याची मागणी करतात.
- पैसे नाही दिले तर तुमचे मित्र नातेवाईक यांना फोन मेसेज करुन तुम्ही डिफॉल्टर आहात म्हणून सांगतात व तुम्हाला पैसे भरण्यास सांगतात. तसेच अश्लिल मेसेज तयार करुन तुमच्या संपर्कातील व्यक्तींना पाठविण्याची धमकी देतात.

➢ प्रतिबंधात्मक उपाय घ्यावयाची काळजी -

- आपण ज्या कंपनीकडून कर्ज घेत आहात ती कंपनी भारतातील आहे का परदेशी ? याची खात्री करावी. तसचे त्या कंपनीला कर्ज देण्याची परवानगी भारत सरकारकडून मिळाली आहे का ? हे तपासावे. कंपनीचे ऑफिस कोठे आहे ? कर्ज देणारी संस्था / कंपनी कोणती आहे ? याची माहिती घ्यावी.
- सदर कंपनी व ॲप बाबत अगोदरच्या लोकांचे **Review** अनुभव काय आहेत ? याची माहिती घ्यावी.
- आपले आधारकार्ड फक्त इनकम टॅक्स भरताना, पॅनकार्ड शी लिंक करताना, गॅस कनेक्शन देतांना, रेशनकार्ड साठी आणि सरकारी योजनांचा लाभ घेताना या पाच ठिकाणीच दयावयाचा असतो. इतर ठिकाणी आधारकार्ड शक्यतो देऊ नये. रहिवाशी पुरावा, फोटो ओळख या साठी इतर कोणकोणते कागदपत्रे चालू शकतात याची माहिती घ्यावी. अनोळखी कंपनी, ॲप, व्यक्ती यांना कागदपत्रे देऊ नये.

- फोन करणारी व्यक्ती मोबाईल नंबरचा वापर करत असेल तर त्यांना लॅण्डलाईन नंबर वरुन फोन करण्यास सांगावे. मोबाईल नंबर व कर्ज देणारी कंपनी, कर्ज देणारे ॲप, बँक अकाऊन्ट यांचा एकमेकांशी काय संबंध आहे याची खात्री करावी.
- कर्ज घेताना ते कर्ज आपण कोणत्या अटी व शर्तींच्या अधीन घेत आहोत ते वाचावे. याबाबत पुढे काही वाद झाला तर तो कोणत्या कोर्टात चालेल याची माहिती घ्यावी व पूर्ण खात्री झाल्यावरच कर्ज रक्कम स्विकारावी.
- रिझर्व बँक इंडियाव्दारे प्रमाणीत ॲप किंवा कंपनीकडूनच लोन घ्यावे.
- आपले गोपनीय दस्तऐवज कागदपत्रे (आधारकार्ड, पॅनकार्ड, बँक डिटेल्स इत्यादी) अनोळखी ॲप वर अपलोड करु नये.
- कोणत्याही लिंक व र क्लिक करुन ॲप डाऊनलोड करु नये.
- तक्रार करताना प्रथम आलेला मेसेज, लिंक, फोन नंबर, कंपनीचे नाव, ॲपचे डिटेल्स, ट्रान्सेक्शन डिटेल्स, बँक अकाऊन्ट याची माहिती **cybercrime.gov.in** या कंम्पलेंट पोर्टल वर दयावी.

➢ Loan App ट्रॅपमध्ये सापडल्यानंतर घ्यावयाची काळजी –

१. प्रथम हे समजून घ्या आपल्यासारखेच सध्या बरेच लोक या लोन ट्रॅपमध्ये फसलेले आहेत. या प्रकाराला घाबरुन न जाता त्याला सामोरे कसे जायचे हे समजुन घ्या.

२. सर्वात प्रथम आपण **Install** केलेले लाने ॲप हे **Uninstall** करावे.

३. सदर ॲप हे **Third Party Apps** असल्यास तुमच्या मोबाईलमधील **Manage Your Google Account** मध्ये जावुन त्यातील **Security Feature** मध्ये जावुन तुम्ही **Download** केलेले **Loan App** तेथुनही **Remove Access** करुन काढुन टाकावे.

Enter Your Google Account

⬇

Manage Your Google Account

⬇

Go To Security Option

⬇

Go To Manage Third Party Access

⬇

Click On Third Party Loan Apps

⬇

Remove Access

⬇

Press Ok

४. तुमच्या व्हाटसॲप **Contacts** असलेल्या सर्वांना **Broadcast List** तयार करुन त्यावर तुमचा फोन हॅक झाला असुन हॅकरने त्यातुन तुमची **Contact List** चोरली असल्याची माहिती त्यांना दयावी. तसेच हॅकर तुमचे व तुमच्या कुटुंबियांचे **Photo Gallery** मधुन **Morph/Edit** करुन **Viral** करित आहे. तरी हॅकरने पाठवलेले **Photo/Videos** ओपन करु नये. तसेच ज्या व्हॉटसॲप नंबरवरुन असे **Photo/Videos** आलेले आहेत. त्या व्हॉटसॲप नंबरला **Report** व **Block** करावे. असा मेसेज तयार करुन तो **Broadcast List** वर सेंड करावा.

Open Your Whatsapp

⬇

Click On Hackers Whatsapp No.

⬇

Click On 3 Dots At Right Side

⬇

Click On More Option & Report

➢ Loan App जागरूकता –

करावे .	करु नये.
• सोशल मिडीया अकाऊन्टचे २ स्टेप व्हेरिफिकेशन करावे. • नेहमी सोशल मिडीया अकाऊन्टवरील प्रोफाईल लॉक करावे. • आपल्या डेबीट व क्रेडिट कार्डची खरेदी मर्यादा निश्चित करुन आंतरराष्ट्रीय ट्रान्झेक्शनचा विकल्प बंद करावा. • अदयावत ॲन्टी व्हायरस / ब्राउझर वापरा आणि **http://** ने सुरु होणा-या **URL** संकेतस्थळाला भेट देणे. • सक्षम पासवर्ड वापरावे आणि प्रत्येक खात्यासाठी वेगवेगळे पासवर्ड वापरावे. • वेळोवेळी कुकीज आणि ब्राउझिंग हिस्ट्री डिलीट करावे. • सायबर क्राईमबाबत त्वरीत तक्रार करावी.	• अनोळखी व्यक्तीची फ्रेंड रिक्वेस्ट स्विकारू नये. • आपला ओटीपी / सीव्हीव्ही / पासवर्ड / पॅनकार्ड / आधारकार्ड इत्यादींचा तपशील अनोळखी व्यक्तींशी शेअर करू नये. • अनोळखी ई-मेल ओपन करू नका तसेच अनोळखी इसमाने पाठवलेले क्यु आर कोड स्कॅन करू नये. • अनोळखी नंबरवरून येणारे व्हिडिओ कॉल स्वीकारू नये. • सोशल मिडियावर सहजरित्या पैसे मिळवण्याच्या प्रलोभनाला बळी पडू नये. • अश्लील व्हिडिओ, फोटो ऑनलाईन डाऊनलोड करू नये. • इंटरनेटवरील खोटया कर्ज योजनांना बळी पडू नये.