Kalupur Bank

The Kalupur Commercial Co-op. Bank Ltd.

SINCE : 1970

Multi State Scheduled Bank

સાયબર ક્રાઈમ

નિવારણ પુસ્તિકા

વિવિધ પ્રકારના સાયબર ક્રાઈમ અને તેનાથી સાવચેત રહેવાના ઉપાય દર્શાવતી માહિતી પુસ્તિકા

THE KALUPUR COMMERCIAL CO-OP BANK LTD.

HEAD OFFICE: KALUPUR BANK BHAVAN, NR. INCOME TAX CIRCLE, ASHRAM ROAD, AHMEDABAD- 380014

પ્રસ્તાવના:

હાલ આપણે એવા યુગમાં જીવી રહ્યાં છીએ જ્યાં ડિજિટલ નવીનતા પ્રગતિને આગળ ધપાવે છે, ત્યારે સાયબર સુરક્ષાના મહત્વને ઓછું દર્શાવી શકાય નહીં. અમે અમારા ગ્રાહકોની નાણાંકીય માહિતી અને ડેટાની સુરક્ષા માટે પ્રતિબદ્ધ છીએ અને અગ્રણી નાણાકીય સંસ્થા તરીકે, આપણી બેંક સાયબર સુરક્ષા જાગૃતિના સર્વોચ્ચ મહત્વને ઓળખીએ છીએ. ટેક્નોલોજીના ઝડપી વિકાસ સાથે, વ્યક્તિઓ અને સંસ્થાઓ સમાન રીતે અનેક સાયબર જોખમોનો સામનો કરી રહ્યાં છે માટે સુરક્ષાના સર્વોચ્ચ ધોરણોને જાળવી રાખવા માટેનું અમારું સમર્પણ માત્ર પ્રતિબદ્ધતા નથી પરંતુ તે એક જવાબદારી છે જેને અમે સર્વોચ્ચ મહત્વ આપીએ છીએ.

આ પુસ્તિકામાં આપેલ માહિતી દ્વારા અમારા મૂલ્યવાન ગ્રાહકો, સાયબર ગુનાઓની અલગ-અલગ મોડસ ઓપરન્ડી વિશે તથા સાયબર ગુનાઓના નિવારણ માટે કેવી સાવચેતી રાખવી તે વિશે .માહિતગાર થશે. અમારી કુશળતા અને અનુભવને આધારે અમે તમને ડિજિટલ ક્ષેત્રને સુરક્ષિત રીતે નેવિગેટ કરવા માટે જરૂરી જ્ઞાન અને સાધનો સાથે સશક્ત બનાવવાનું લક્ષ્ય રાખીએ છીએ.

આ માર્ગદર્શિકા સામાન્ય સાયબર જોખમોને સમજવાથી માંડીને વ્યક્તિગત અને નાણાકીય માહિતીને સુરક્ષિત રાખવા માટે શ્રેષ્ઠ પ્રયાસો અમલમાં મૂકવા તેમજ તમને સાયબર ગુનેગારો સામે તમારા સંરક્ષણને મજબૂત કરવા માટે પગલાં લેવા માટે યોગ્ય આંતરદૃષ્ટિથી સજ્જ કરે છે. તો ચાલો આપણે અને આપણી-આવનારી પેઢીઓ માટે ડિજિટલ ક્રિયાપ્રતિક્રિયાઓની સુરક્ષા અને અખંડિતતાને સુનિશ્ચિત કરીને તકેદારી અને સુરક્ષાની સંસ્કૃતિને પ્રોત્સાહન આપીએ.

આવો,સાથે મળીને આપણે વધુ સુરક્ષિત ડિજિટલ ભારતનું ભવિષ્ય બનાવીએ.

કાલુપુર બેંક આપણી પોતાની બેંક

Head Office: "Kalupur Bank Bhavan"
Nr.Income Tax Circle, Ashram Road,
Ahemdabad-380014

Phone: 079-27582020 to 26
Email: info@kalupurbank.com
Website: www.kalupurbank.com

અનુક્રમણિકા

માહિતી	પેજ નં.

સાયબર ક્રાઇમ એટલે શું?..4
સાયબર ક્રાઇમ થવા પાછળના કારણો...5
સાયબર ક્રાઇમના મુખ્ય પ્રકારો..6
⇒ સાયબર બુલીંગ , હેકિંગ.. 7
⇒ સોશીયલ મિડીયા ફ્રોડ, ડેટા થેફ્ટ, માલવેર / રેન્સમવેર..................................8
⇒ ફાયનાન્સીયલ (નાણાંકીય) ફ્રોડ..9
સાયબર ક્રાઇમ મોડસ ઓપરન્ડી...10
⇒ ન્યુડ વિડીયો કોલીંગ ફ્રોડ (Sextortion)..11
⇒ ઇન્સ્ટન્ટ લોન એપ ફ્રોડ..12
⇒ બનાવટી લિન્ક (Phishing Link)..13
⇒ ફેક કોલ (Vishing Call)...14
⇒ ઓનલાઇન સેલીંગ પ્લેટફોર્મ ફ્રોડ..15
⇒ સ્ક્રિન શેરીંગ એપ / રીમોટ એક્સેસ એપ ફ્રોડ...16
⇒ કસ્ટમર કેર ફ્રોડ..17
⇒ SIM સ્વેપ / SIM ક્લોનિંગ ફ્રોડ..18
⇒ અજાણી / અનવેરીફાઇડ મોબાઇલ એપ્લીકેશન ફ્રોડ................................ 19
પોન્ઝી સ્કીમ (ઓનલાઈન ઇન્વેસ્ટમેન્ટ ફ્રોડ)...20
સાયબર ક્રાઇમ ની જાણ કઈ રીતે કરવી (હેલ્પ લાઈન તથા પોર્ટલ)........................ 21
સાયબર સેલના પોર્ટલ પર ફરિયાદ નોધાવવાની સંપૂર્ણ પ્રક્રિયા 22
સાયબર ક્રાઈમ સામે સલામતીની ટીપ્સ..25
સાયબર ક્રાઈમની જાણ બેંક ને કરવી 26
સાયબર ક્રાઈમ સેલ ની યાદી અને સંપર્ક માહિતી..27

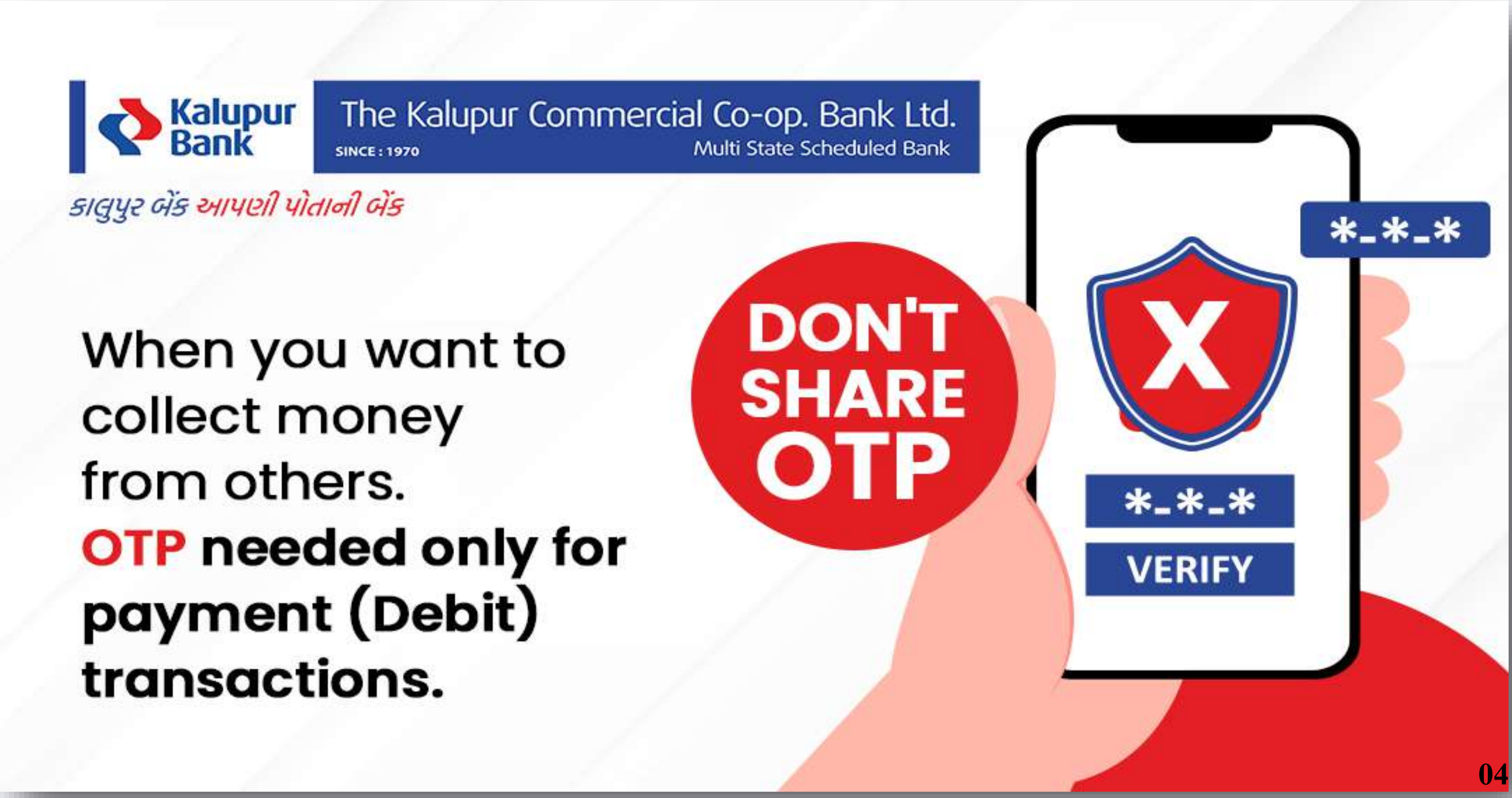
સાયબર ક્રાઇમ એટલે શું?

સામાન્ય રીતે સાયબર ક્રાઈમ ને નીચે પ્રમાણે વર્ણવી શકાય.

⇒ **સાયબર ક્રાઇમ એટલે કોઈપણ ગુનાહિત પ્રવૃત્તિ જેમાં મોબાઇલ, કોમ્પ્યુટર, લેપટોપ, ટેબલેટ દ્વારા ઇન્ટરનેટના માધ્યમ વડે કોઇપણ પ્રકારની લાલચ, છેતરપીંડી, ધાક-ધમકી, નાણાકીય ફ્રોડ, અપમાનજનક ભાષાનો પ્રયોગ, પાસવર્ડ કે અન્ય ડિજિટલ ડેટાની ચોરી કરવી જેવા ગુના એટલે સાયબર ક્રાઇમ.**

⇒ **કમ્પ્યુટર, ઇન્ટરનેટ વાળુ કોઈ પણ સાધન કે ઇન્ટરનેટ નેટવર્કના ઉપયોગ થી થતી ગુનાહિત પ્રવૃત્તિ.**

⇒ **મોટાભાગના સાયબર અપરાધો સાયબર અપરાધીઓ દ્વારા નાણા મેળવવા માટે કરવામાં આવે છે, ત્યારે કેટલાક સાયબર અપરાધો કમ્પ્યુટર અથવા માહિતીનો નાશ કરવો, કોઈને ઓનલાઇન ધમકી આપવી, જાતીય શોષણ બદનામીનું ડિજિટલ માધ્યમ બની રહ્યું છે.**



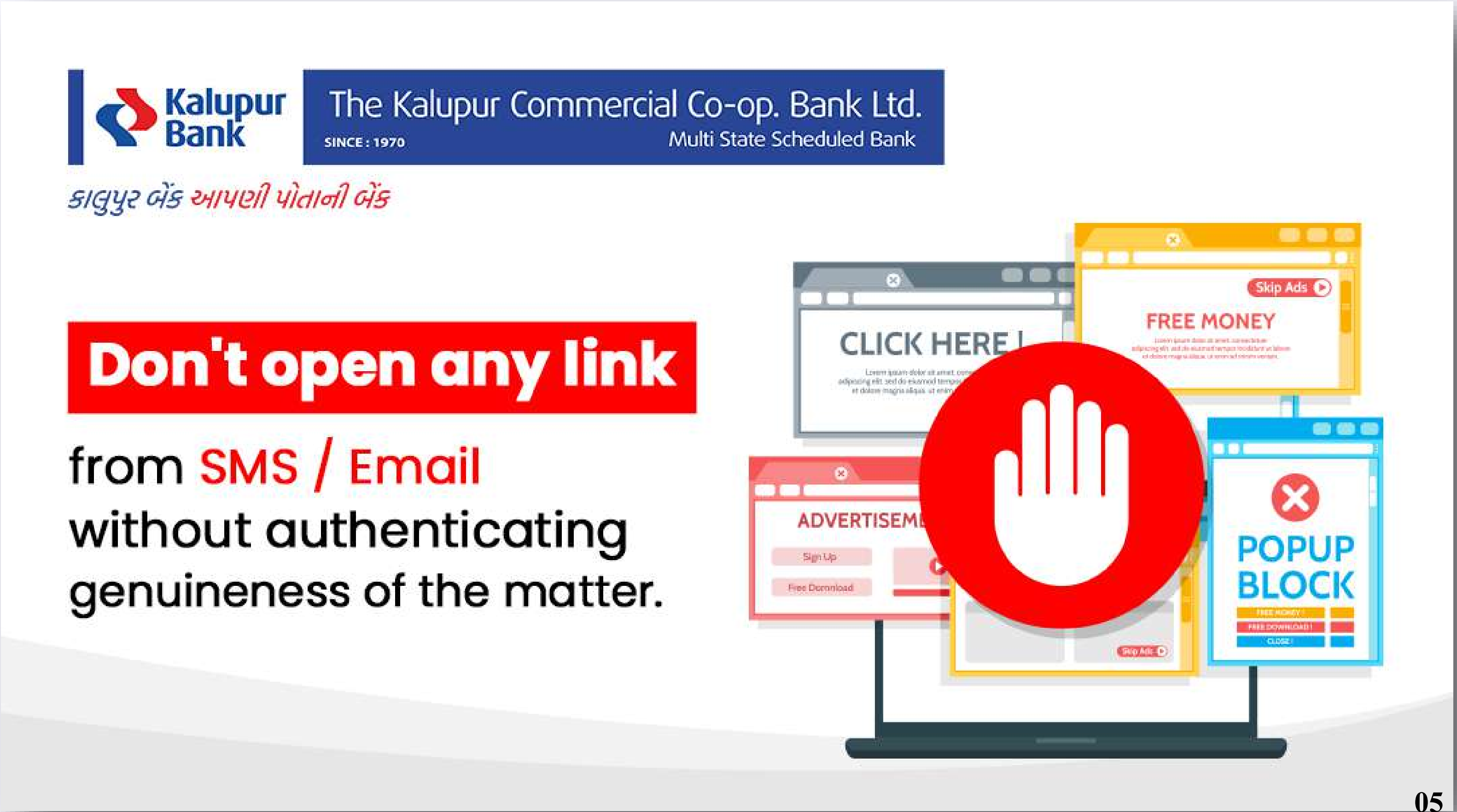
સાયબર ક્રાઇમ થવા પાછળના મુખ્ય કારણ

સામાન્ય રીતે સાયબર ક્રાઈમ નીચેની બાબતો ની લીધે થતા હોય છે તેમજ સાયબર ગુનેગારો નીચેની બાબતો નો લાભ લઇ ગુનો આચરતા હોય છે.

⇒ **ડર:**
નાગરીકો ઘણી વખત ડરમાં આવીને નાણાંકિય ચુકવણી કરી દેતા હોય છે અથવા તો અજાણી લિન્ક પર ક્લિક કરી માહિતી આપતા હોય છે અને છેતરપીંડીનો ભોગ બનતા હોય છે.

⇒ **લાલચ:**
નાગરીકો ઘણી વખત ઇનામ, ઓફર વગેરે જેવા ખોટા મેસેજ કે લિન્કની લાલચમાં આવીને ખરાઇ કર્યા વગર ક્લિક કરી માહિતી તેમજ નાણાંની ચુકવણી કરી છેતરપીંડીનો ભોગ બને છે.

⇒ **આળસ:**
નાગરીકો ઘણી વખત આળસમાં આવી ને મેસેજ કે ઇ-મેઇલની ખરાઇ કર્યા વગર જ તુરંત જ માહિતી આપે છે અથવા તો પીન નં., ઓ.ટી.પી. વગેરે જણાવી છેતરપીંડીનો શીકાર બનતા હોય છે.



સાયબર ક્રાઇમના પ્રકારો

સાયબર ગુનેગારો સાયબર ક્રાઈમ અનેક રીતે આચરતા હોય છે, જેને નીચે મુજબનાં ભાગોમાં વર્ગીકૃત કરી શકાય. જેની વિસ્તૃત માહિતી મેળવીશું.

⇒ સાયબર બુલીંગ

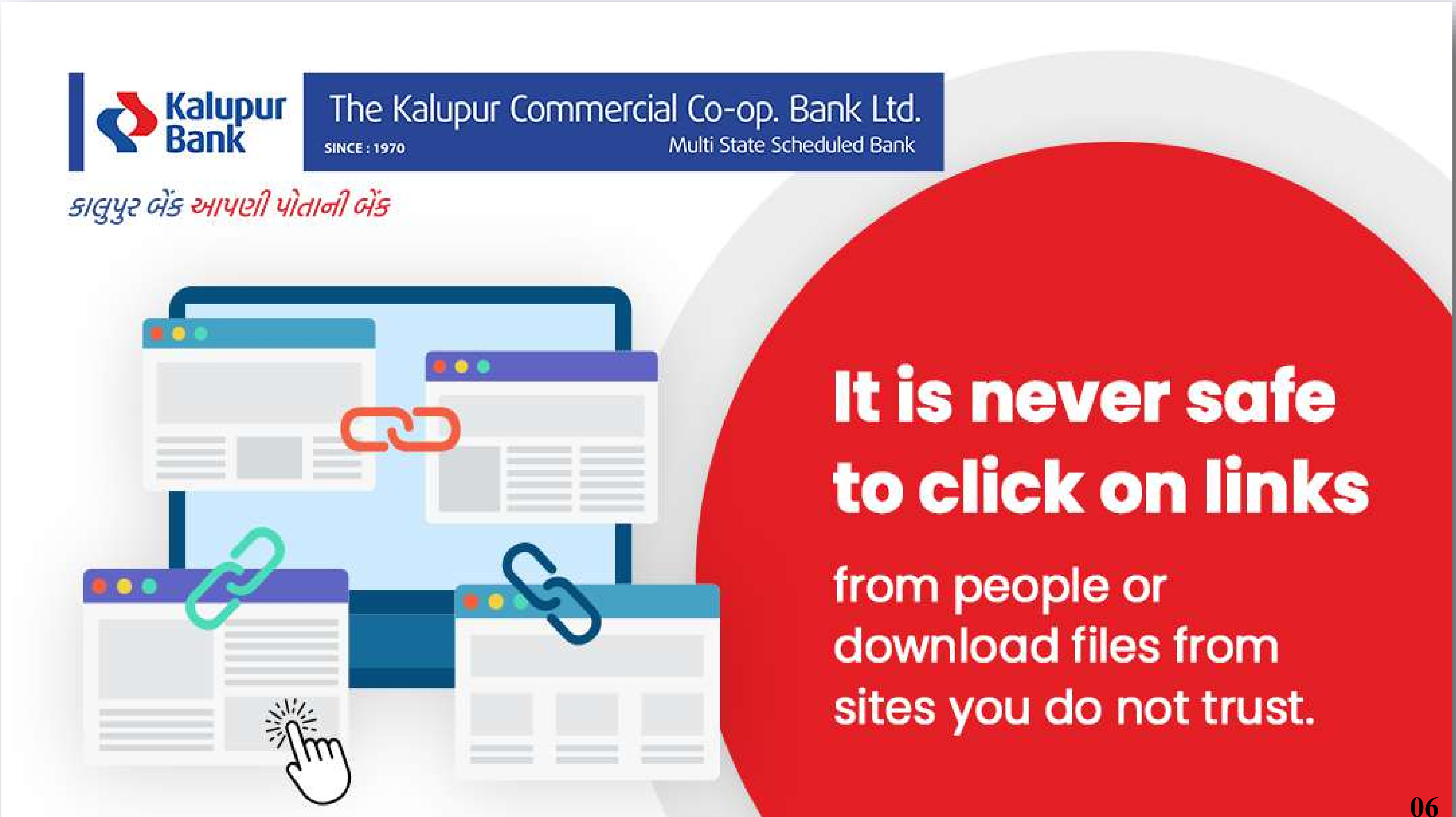
⇒ હેકિંગ

⇒ સોશીયલ મીડીયા ફ્રોડ

⇒ ડેટા થેફ્ટ

⇒ માલવેર / રેન્સમવેર

⇒ ફાયનાન્સીયલ ફ્રોડ



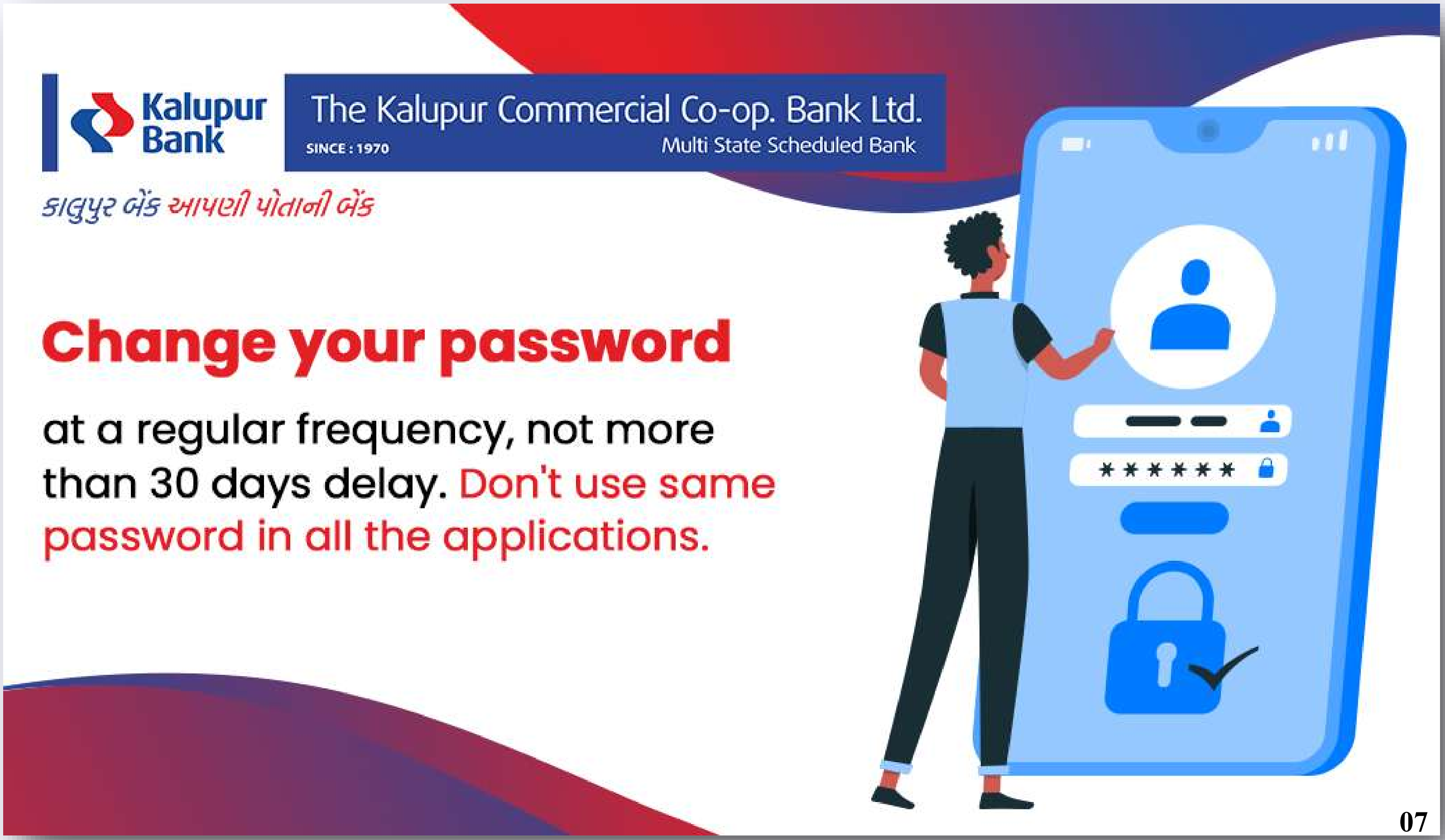
સાયબર ક્રાઇમના પ્રકારો

⇒ સાયબર બુલીંગ

સોશિયલ મીડિયાની આજની દુનિયામાં, ભારતનો લગભગ દરેક યુવક વિવિધ પ્રકારના સોશિયલ મીડિયામાં સક્રિય છે. આવી સ્થિતિમાં કોઈપણ વ્યક્તિ કોઈપણ છોકરા કે છોકરીને માનસિક રીતે પરેશાન કરે છે.
જેમ કે દુરુપયોગ, જાતીય શોષણ (sexual abuse), ધમકી આપવી અથવા સોશિયલ મીડિયા પર કોઈની છબી ખરાબ કરવાનો પ્રયાસ કરવો. આ બધા સાયબર ધમકી હેઠળ આવે છે જે સાયબર ક્રાઇમ છે.

⇒ હેકિંગ

હેકિંગ એ એવી પદ્ધતિ છે કે જેના દ્વારા ગુનેગાર તમારી પરવાનગી વગર તમારી અંગત માહિતી ચોરી લે છે. જેનો ઉપયોગ તે તમને નુકસાન પહોંચાડવા અથવા તમારી મહત્વપૂર્ણ માહિતી અન્યને વેચવા માટે કરે છે. આ સિવાય હેકર તમારા સોશિયલ મીડિયાને સોફ્ટવેર દ્વારા હેક કરે છે.
મોબાઈલ કે કોમ્પ્યુટર હેકિંગ અને પછી તેનો ઉપયોગ ખોટા હેતુ માટે કરવો. તમારી પરવાનગી વગર તમારી બેંક માહિતી મેળવવી, આ બધું હેકિંગ હેઠળ આવે છે.



સાયબર ક્રાઇમના પ્રકારો

⇒ **સોશીયલ મિડીયા ફ્રોડ:**

આજકાલ લોકો Social Media નો ભરપુર ઉપયોગ કરી રહા છે. કોઇ વેપાર માટે તો કોઈ મનોરંજન માટે, કોઇ ગપશપ કરવા માટે કે નવા મિત્રો બનાવવામાટે WhatsApp, Facebook, Instagram, Twitter, YouTube જેવી એપ્લીકેશન વડે સતત એકબીજાના સંપર્કમાં રહેતા હોય છે.

પરંતુ અહીં પણ તમારી સાથે છેતરપીંડી કરવા માટે ઘણા અસામાજીક સાયબર તત્વો તમને મુશ્કેલીમાં મૂકી શકે છે. જેમ કે, Social Media પર અન્ય વ્યક્તિના નામે Fake પ્રોફાઇલ બનાવવી/ પ્રોફાઇલ પેજ હેક કરવા અન્ય કોઇ વ્યક્તિના ફ્રોટો કે વિડીયો બિનઅધિકૃત રીતે અપલોડ કરવા બિભત્સ ભાષા, સાહિત્ય કે પોર્નોગ્રાફી Fake News કે ખોટી અફવા ફેલાવવી ધર્મ, જાતિ, ભાષા કે પ્રાંતને નિશાન બનાવી અન્યની લાગણીને ઠેસ પહોંચાડવી તેમજ તે પ્રકારની માહિતી, ફોટા કે વિડીયો અપલોડ કરવા, ટેગ અથવા શેર કરવુ પણ ગંભીર ગુનો બને છે.

⇒ **ડેટા થેફ્ટ:**

એકદમ સરળ શબ્દોમાં કહીએ તો, કોઇપણ વ્યક્તિનો અંગત, સંસ્થા, પ્રાઇવેટ કંપની કે સરકારી એકમોમાંથી વેબસાઇટ, કોમ્પ્યુટર, પેનડ્રાઇવ, ઇમેલ આઇ.ડી.ના માધ્યમથી ડિજિટલ ડેટા ચોરી કરવામાં આવે છે, જેને ડેટા થેફ્ટ કહેવાય છે.

⇒ **માલવેર / રેન્સમવેર**

Malware / Ransomware એક પ્રકારનો દુષિત સોફ્ટવેર છે. જે આપમેળે જ ઇન્ટરનેટ અને ઈ-મેલથી તમારા કમ્પ્યુટરમાં આવી જાય છે, જેના કારણે તમારા કમ્પ્યુટરની તમામ ફાઇલ્સ Encrypt થઇ જાય છે.
આ વાયરસ તમારી સિસ્ટમની અમુક ફાઇલ કે ફોલ્ડર, જે તમે રોજ યુઝ કરતા હોવ, તે શોધે છે.
તે કમ્પ્યુટરમાં ફ્રીક્વન્ટલી યુઝડ ફાઇલ અને લાસ્ટ મોડીફાઇડ ફાઇલ ચેક કરે છે અને તે ફાઇલનું ફોર્મેટ ચેન્જ કરી નાંખે છે.
આ કારણે જ્યારે તમે તે ફાઇલ કે ફોલ્ડર ફરીથી ઓપન કરવા જાઓ તો ખોલી નહીં શકો, ઘણા કિસ્સાઓમાં યૂઝર્સ પોતાની ફાઇલ-ફોલ્ડર શોધી પણ નથી શકતા. આની પાછળનું કારણ છે Malware / Ransom-ware વાયરસ. આ વાયરસની કોઇ એક પેટર્ન નથી. તે અલગ-અલગ સર્વરથી, અલગ-અલગ લીંકથી તમારી સીસ્ટમ, સર્વર કે ડિવાઇઝ પર હાવી થઇ શકે છે. દાત:

Your personal files are encrypted

кун хороох хохххх ххххх—**Decrypt**

⇒ **<u>ફાયનાન્સીયલ (નાણાકીય) ફ્રોડ:</u>**

પહેલાંના સમયમાં હાથમાં છરી જેવા હથિયાર લઇને અસામાજીક તત્વો લુંટ ચલાવતા, પરંતુ હવે તમારા ડેબીટ કાર્ડ કે ક્રેડિટ કાર્ડમાં આયોજનપુર્વક OTP (વન ટાઇમ પાસવર્ડ)ના માધ્યમથી લાખો-કરોડો રૂપિયાની ઉઠાંતરી ના કિસ્સાઓ સામે આવ્યા છે.

નાગરિકોને ફોન ઉપર બેંક મેનેજર/કર્મચારી કે RBI ના અધિકારી હોવાની નકલી ઓળખ આપીને વિશ્વાસ કેળવી તેમના મોબાઇલ ફોન પર આવેલા OTP ઉપરાંત ડેબીટ/ ક્રેડીટ કાર્ડ જેવી મહત્વપુર્ણ માહિતી મેળવી નાગરિકોના ખાતામાંથી રકમ ઉપાડી લેવામાં આવે છે.

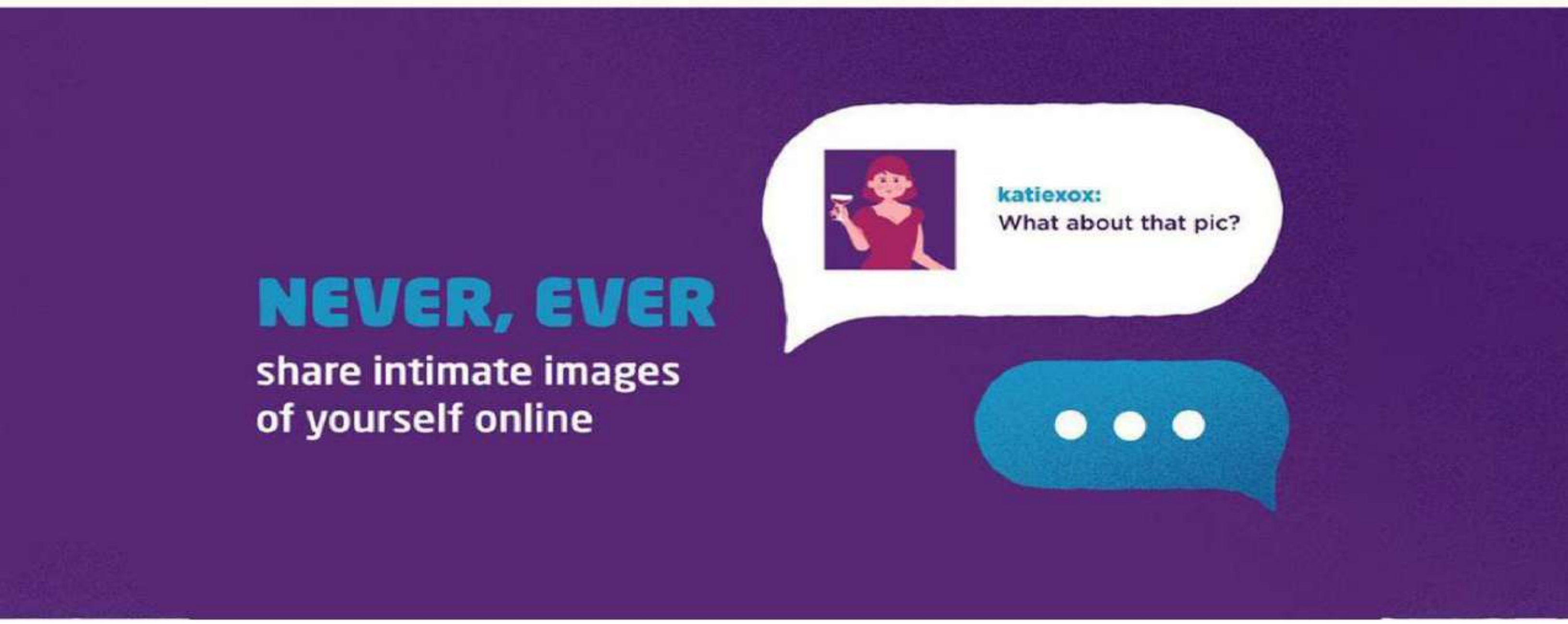
ગુનેગારો વિવિધ સાયબર ગુનાઓ આચરવા માટે વિવિધ પ્રકારની રીતો અપનાવાવતા હોય છે જેની માહિતી હવે મેળવીશું.

- ન્યુડ વિડીયો કોલીંગ ફ્રોડ (Sextortion)
- ઇન્સ્ટન્ટ લોન એપ ફ્રોડ
- બનાવટી લિન્ક (Phishing Link)
- ફેક કોલ (Vishing Call)
- ઓનલાઇન સેલીંગ પ્લેટફોર્મ ફ્રોડ
- સ્ક્રિન શેરીંગ એપ / રીમોટ એક્સેસ એપ ફ્રોડ
- કસ્ટમર કેર ફ્રોડ
- SIM સ્વેપ / SIM ક્લોનિંગ ફ્રોડ
- અજાણી / અનવેરીફાઇડ મોબાઇલ એપ્લીકેશન ફ્રોડ

ન્યુડ વિડીયો કોલીંગ ફ્રોડ (Sexortion)

મોડસ ઓપરન્ડી

- સોશીયલ મિડીયા સાઇટ્સ જેમ કે ફેશબુકમાં સાયબર ગઠીયા ફેક પ્રોફાઇલ બનાવી તમને ફ્રેન્ડ રીક્વેસ્ટ મોકલે છે.
- ફ્રેન્ડ રીક્વેસ્ટ એક્સેપ્ટ કરતા સાયબર ગઠીયા ધીમે ધીમે ચેટ શરૂ કરે છે સાથે સાથે તમારા ફ્રેન્ડ સાથે પણ જોડાઇ જાય છે.
- ચેટમાં વાતો કરી વિસ્વાસમાં લઇને તમારો વ્હોટ્સએપ નંબર માંગે છે કા તો એમનો વ્હોટ્સએપ નંબર આપે છે. વિડીયો કોલ કરવા માટે કહે છે જેમાં સેક્સ વિડીયો કોલ માટે કહે છે.
- આમ કરવાથી ગઠીયાઓ વિડીયો રેકોર્ડીંગ એપ્લીકેશનથી રેકોર્ડ કરી વિડીયો બનાવે છે અને નાણાની માંગણી કરે છે.



સાવચેતી

- કોઇ પણ રૂપીયાની ચુકવણી કરવી નહી અને આવા પ્રકારની પ્રોફાઇલની ફ્રેન્ડ રીક્વેસ્ટ એક્સેપ્ટ કરશો નહી અને વાતચીત પણ કરવી નહી.

ઇન્સ્ટન્ટ લોન એપ ફ્રોડ

ઇન્સ્ટન્ટ લોન એપ દ્વારા વધુ વ્યાજ દરથી ટુંકા સમયગાળા માટે લોન આપવાનું જણાવે છે.

આવી એપ ડાઉનલોડ કર્યા બાદ ઇન્સ્ટોલેશન સમયે ફોટા તેમજ કોન્ટેક્ટને એલાઉ કરતા તમારો ડેટા મેળવી લે છે.

ત્યારબાદ તમારા ફોટાનો દુરઉપયોગ કરી બદનામ કરી છેતરપીંડી આચરે છે.

સાવચેતી

⊙ સાવચેતી:- આવી બોગસ એપ ડાઉનલોડ કરવાનું ટાળો.

બનાવટી લિન્ક (Phishing Link)

મોડસ ઓપરન્ડી

- સાયબર ગઠીયાઓ બેન્ક , ઇ–કોમર્સ કે સરકારી વેબસાઇટ જેવી જ બનાવટી વેબસાઇટ બનાવે છે.
- બનાવટી વેબસાઇટની લિન્ક એસ.એમ.એસ.,ઇ–મેઇલ,વ્હોટ્સએપ,સોશીયલ મિડીયા દ્વારા લાલચ આપી મોકલવામાં આવે છે.
- આવી લિન્કને ખરાઇ કર્યા વગર જ લાલચમાં આવીને ક્લિક કરતા જે વેબસાઇટ ઓપન થાય છે તે ઓરીજીનલ દેખાતી વેબસાઇટ જેવી લાગતી હોય છે પરંતુ તે ઓરીજીનલ હોતી નથી.
- નાગરીકોની બેન્ક ની તેમજ પર્સનલ માહિતી આવી બનાવટી લિન્ક દ્વારા ડેટા એન્ટ્રી હેઠળ મેળવી સાયબર ગઠીયાઓ આ માહિતીનો દુરઉપયોગ કરી છેતરપીંડી કરે છે.

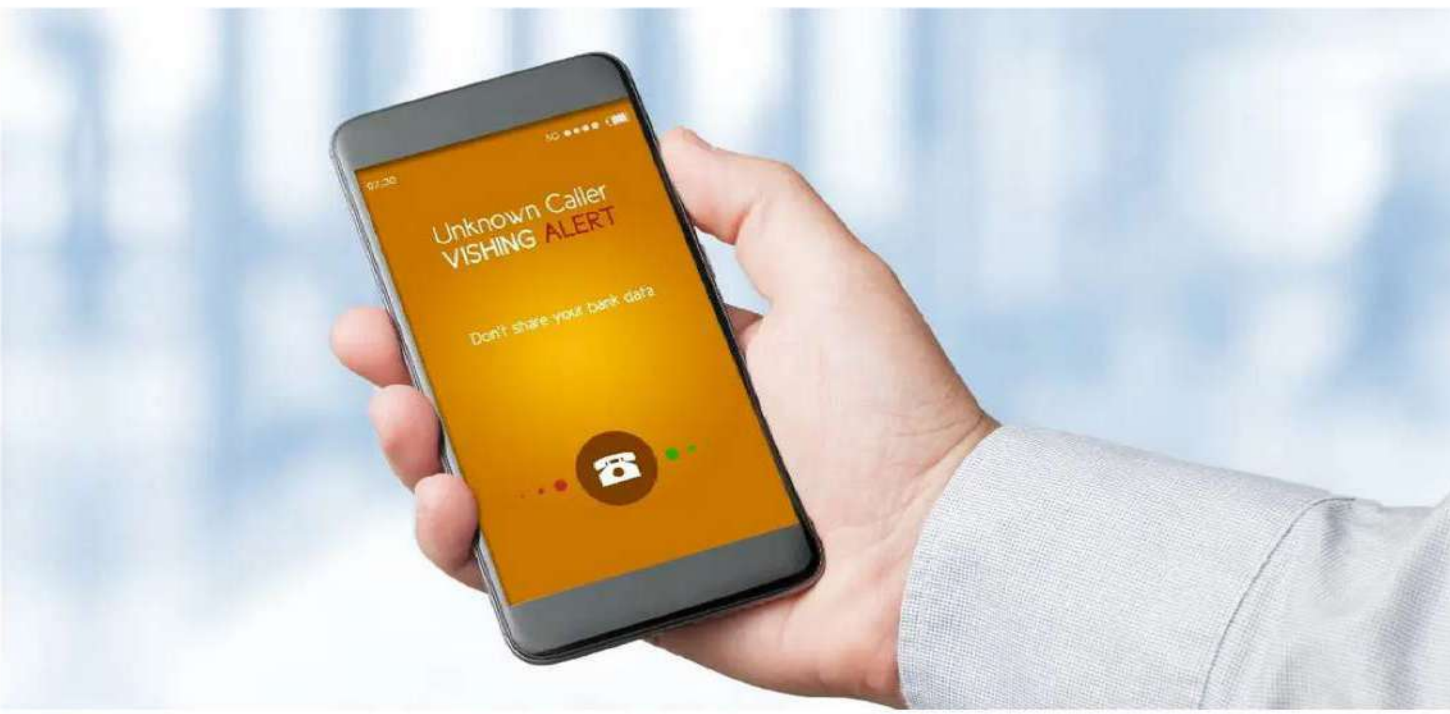
સાવચેતી

- અજાણી લિન્ક પર ક્લિક ન કરવું જોઈએ.
- વેબસાઇટની વિગતો ચકાસવા માટે ખાસ કાળજી લેવી.
- આવી લિન્ક ભુલ થી પણ ઓપન થઇ જાય તો બેન્ક ની વિગત,પર્સનલ માહિતી દાખલ કરશો નહિ.

ફેક કોલ (Vishing Call)

મોડસ ઓપરન્ડી

- સાયબર ગઠીયાઓ ફોન કોલ કરી બનાવટી બેક્ક કર્મચારી/ કંપેની એક્ઝ્યુકીટીવ/ઇન્સ્યોરન્સ એજન્ટ/સરકારી કર્મચારી બની તમારી માહિતી જેવી કે નામ, જન્મ તારીખ વગેરે જણાવી વિશ્વાસમાં લઇ તમારી બેન્કની વિગતો મેળવી લે છે.
- ઘણા કિસ્સાઓમાં આવા કોલ કરી તમારુ એકાઉન્ટ બંધ થઇ જશે, પેનલ્ટી લાગશે, એકાઉન્ટ એક્ટીવ કરવુ તેમજ સીમ કાર્ડ બંધ થઇ જશે તેમ કહી નાણાકીય છેતરપીંડી કરે છે.



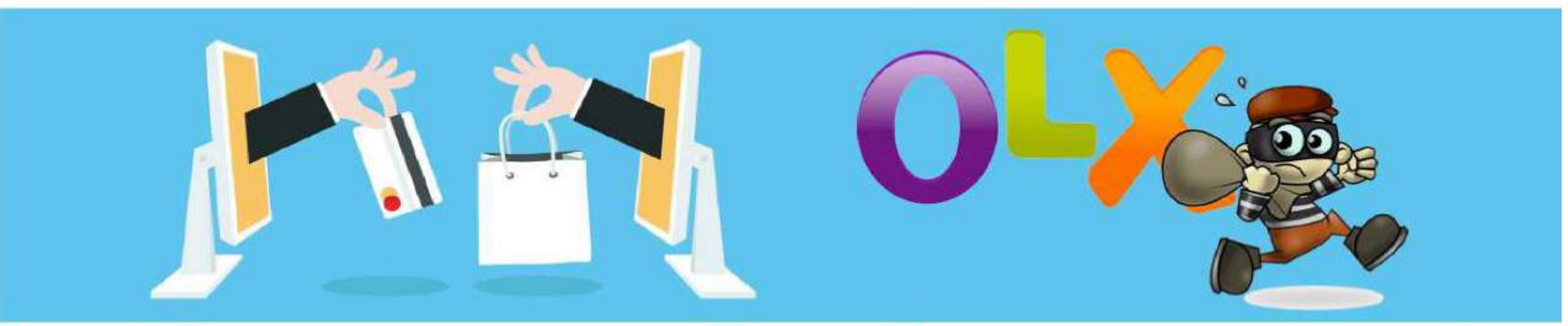
સાવચેતી

- બેન્ક / ફાઇનાન્સીયલ ઇન્સ્ટીટ્યુટ / કોઇપણ અધિકૃત સંસ્થા ક્યારેય બેન્ક ની વિગતો જેવી કે પાસવર્ડ, કાર્ડ ડિટેલ્સ, સીવીવી, ઓટીપી કે પિન માંગતી નથી.

ઓનલાઇન સેલીંગ પ્લેટફોર્મ ફ્રોડ

મોડસ ઓપરન્ડી

- સાયબર ગઠીયા ઓનલાઇન સેલીંગ પ્લેટફોર્મ જેવા કે OLX એપ્લિકેશન દ્વારા ખરીદદાર બની કોઇ પણ ભાવે તમારી પ્રોડક્ટ ખરીદવા તૈયાર થાય છે.
- ત્યારબાદ તે પ્રોડક્ટ ખરીદવા માટે તમને નાણાં ચૂકવવાને બદલે, તેઓ UPI એપ દ્વારા "request money"નો ઉપયોગ કરે છે અને તેમના જણાવ્યા મુજબ કાર્યવાહી કરતા તમારા બેંક ખાતામાંથી નાણાં તેમના એકાઉન્ટમાં જતા રહે છે
- OLX જેવી એપ્લીકેશન પર સાયબર ગઠીયાઓ સેલર બની વસ્તુની સસ્તી કિમંતની એડ મુકી આર્મી મેન બની બનાવટી આઇ કાર્ડ બતાવી વિશ્વાસમાં લઇ કુરીયર કરવાના બહાને એડવાન્સ પેમેન્ટ કરાવી છેતરપીંડી કરે છે.
- OLX જેવી એપ્લીકેશન પર સાયબર ગઠીયાઓ બાયર બની તમે ઉંચો ભાવ મુકો તો પણ તુરંત જ ખરીદ કરવા તૈયાર થઇ જાય છે અને તમને નાણાની ચુકવણી કરવા માટે કોડ સ્કેન કરવા તેમજ રીક્વેસ્ટના માધ્યમનો ઉપયોગ કરી તમને નાણા આપવાને બદલે મેળવી લેતા હોય છે.



સાવચેતી

- ઓનલાઈન પ્રોડક્ટ્સ માટે નાણાકીય વ્યવહારો કરતી વખતે સાવચેત રહેવું જોઈએ.
- હંમેશા યાદ રાખો, પૈસા મેળવવા માટે તમારો PIN / પાસવર્ડ ક્યાંય દાખલ કરવાની જરૂર નથી.
- જો UPI અથવા અન્ય કોઈ એપ્લિકેશન તમને વ્યવહાર પૂર્ણ કરવા માટે તમારો PIN દાખલ કરવાનું કહે છે તો તેનો અર્થ એ કે તમે તેને પ્રાપ્ત કરવા ને બદલે પૈસા મોકલવાનું કામ કરી રહ્યા છો.

મોડસ ઓપરન્ડી

- છેતરપિંડી કરનારા તમને સ્ક્રીન શેરિંગ એપ્સ ડાઉનલોડ કરવા માટે ફસાવે છે જેના દ્વારા તેઓ તમારો મોબાઇલ કે કોઇપણ ડીવાઇસને સરળતાથી જોઇ શકે છે.
- ત્યારબાદ તેઓ તમારા મોબાઇલ પર આવેલ ઓ.ટી.પી. કે તમારી ઇન્ટરનેટ બેંકિંગ કે પેમેન્ટ એપ્લિકેશન્સન ને એક્સેસ કરે છે અને તમારા ખાતામાંથી રૂપીયા ઉપડી જાય છે.

Stop fraudsters
from taking control of your phone using screen sharing!

સાવચેતી

- આવી કોઇ એપ્લીકેશન કે લાલચમાં આવીને કોઇ લિન્ક ખોલી અજાણી એપ્લીકેશન ઇન્સ્ટોલ કરવી નહિ.

કસ્ટમર કેર ફ્રોડ

મોડસ ઓપરન્ડી

- એવુ ધ્યાનમાં આવેલ છે કે નાગરીકો સર્ચ એન્જીનનો ઉપયોગ કરી બેક્ક કસ્ટમર કેર નંબર, ઇન્સ્યોરન્સ કંપની, આધાર અપડેશન સેન્ટર વગેરે સર્ચ કરે છે અને ખરાય કર્યા વગર દર્શાવેલ કોન્ટેક્ટ નંબર મેળવે છે.
- નાગરીક આવા નંબર પર કોલ કરે છે અને તમારી બેક્કની માહિતી મેળવી લેવામાં આવે છે.
- આવા નંબરને અસલી માનીને, લોકો તેમની તમામ સુરક્ષિત વિગતો આપે છે અને છેતરપિંડીનો શિકાર બને છે.

સાવચેતી

- સર્ચ અન્જીનનો ઉપયોગ કરીકસ્ટમર કેર નંબર મેળવવાનું ટાળવુ જોઇએ.
- બેન્ક કે કંપનીની ઓરીજીનલ ઓફીશીયલ વેબસાઇટ પરથી જ કસ્ટમર કેર નંબર મેળવવો જોઇએ.

SIM સ્વેપ / SIM ક્લોનિંગ ફ્રોડ

મોડસ ઓપરન્ડી

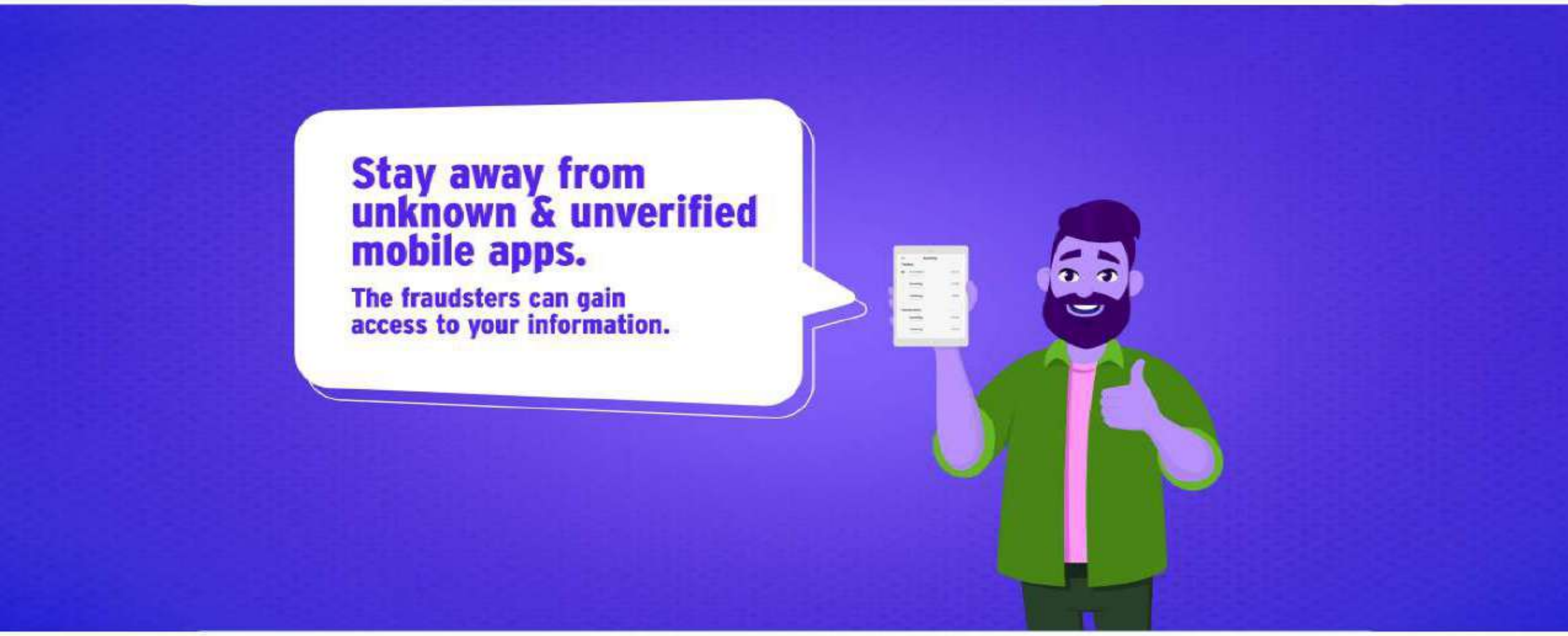
- એકાઉન્ટ ડીટેલ્સ અને ઓથેન્ટીકેશન મોબાઇલ નંબર સાથે સંકળાયેલ હોય છે જેથી સાયબર ગઠીયા ઓટીપી માટે ડુપ્લીકેટ સિમ કાર્ડનો ઉપયોગ કરતા હોય છે.
- સાયબર ગઠીયા નાગરીકોને કોલ કરી મોબાઇલ નેટવર્ક કર્મચારી બની નાગરીકોને 3જી માંથી 4જી કાર્ડ કન્વર્ટ કરવાના બહાને માહિતી મેળવી લે છે અને છેતરપીંડી આચરે છે.

સાવચેતી

- સિમ કાર્ડ સંબંધિત ઓળખ કે માહિતી શેર કરશો નહીં.
- જો તમારા મોબાઇલમાં નેટવર્ક જતુ રહે તો તાત્કાલીક મોબાઇલ ઓપરેટરનો સંપર્ક કર્વો અને ખાત્રી કરવી જોઇએ કે ડુપ્લીકેટ સિમ કાર્ડ બનાવવામાં આવેલ નથી ને જો તેવુ થાય તો તાત્કાલીક બંધ કરાવવુ જોઇએ.

મોડસ ઓપરન્ડી

- સાયબર ગઠીયા અજાણી એપ્લીકેશન ડાઉનલોડ કરાવી તમારા મોબાઇલ ડીવાઇસ, લેપટોપ, કમ્પ્યુટરનું એક્સેસ મેળવી લે છે.
- આવી એપ્લીકેશનની લિન્ક સામાન્ય રીતે એસ.એમ.એસ./સોશીયલ મિડીયા/વ્હોટ્સએપ જેવી મેસેન્જર એપ દ્વારા મોકલવામાં આવે છે.
- આવી લિન્ક ઓરીજીનલ લિન્ક જેવી દેખાતી હોય છે પરંતુ તે માસ્ક કરેલ હોય છે અને ક્લિક કરતા બનાવટી એપ્લીકેશનને ડાઉનલોડ કરવા તરફ દોરી જાય છે.
- જેવી આવી એપ્લીકેશન ડાઉનલોડ કરવામાં આવે છે તેવુ ગઠીયા દ્વારા તમારા ડિવાઇસનું એક્સેસ મેળવવામાં આવે છે અને છેતરપીંડી આચરવામાં આવે છે.



સાવચેતી

- ક્યારેય આવી લિંક ઓપન કરી એપ્લીકેશન ડાઉનલોડ કરવી નહિ.

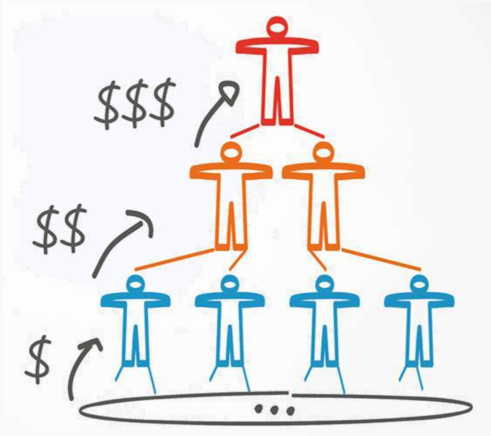
પોન્ઝી સ્કીમ (ઓનલાઈન ઇન્વેસ્ટમેન્ટ ફ્રોડ)

મોડસ ઓપરન્ડી

⇒ પોન્ઝી સ્કીમ એ ફ્રોડ માટેનું સુ-વ્યવસ્થિત માધ્યમ છે. જેમાં રોકાણકારો ને વિવિધ સ્કીમ માં ઓછા જોખમ પર વધુ રીટર્ન આપવાની લાલચ આપવામાં આવેછે. આ સ્કીમમાં સામાન્યરીતે વધુને વધુ લોકોને જોડવા માટે મલ્ટીલેવલ માર્કેટિંગ નો સહારો પણ લેવામાં આવેછે. તેમજ વિવિધ એપ્સનો ઉપયોગ કરવામાં આવે છે.

⇒ આ પ્રકારની સ્કીમ માં શરૂઆતમાં લોકોને રોકાણ કરાવી ને થોડું ઘણું રીટર્ન આપવામાં આવેછે જેથી તે વ્યક્તિ લાલચમાં આવીને વધુમાં વધુ રોકાણ કરે.

⇒ આ સ્કીમમાં વધારે સભ્યોને જોડીને વધારે લાભ મેળવે તે રીતે લાલચ આપવામાં આવે છે અને શરૂઆતમાં જેમ—જેમ નવા સભ્યો જોડાય તેમ તેમ તેમના રોકાણમાંથી જુના સભ્યોને થોડું ઘણું રીટર્ન આપવામાં આવેછે. અને જયારે મોટી રકમ એકત્રિત થાય ત્યારે આખી પેઢી અથવા ફ્રોડ કંપની પૈસા લઈને ફરાર થઇ જાય છે.



સાવચેતી :

⇒ રોકાણ કરવા માટે હમેશા સેબી અને RBI માન્ય નાણાંકીય સંસ્થાઓ ની પ્રમાણિત એપ્લીકેશનનો જ ઉપયોગ કરવો.

⇒ ચેનલ માર્કેટિંગ કે પિરામીડ સ્કીમની લાલચમાં ન આવવું તેમજ લાલચમાં આવીને અન્ય ને ના જોડવા.

⇒ ઓછા જોખમે ખુબજ વધુ રીટર્ન આ સ્કીમમાં ફસાવવા માટેનું કોમન માધ્યમ હોય છે.

સાયબર ફ્રોડ ની જાણ

જો આપની સાથે ઓનલાઇન નાણાંકિય ફ્રોડ કે અન્ય સાયબર ક્રાઇમ થાય છે તો તમે બે રીતે તમારી ફરિયાદ નોંધાવી શાકો છો. 1. સાયબર ક્રાઇમ હેલ્પલાઇન પર તથા 2.સાયબર ક્રાઇમ પોર્ટલ પર.

1. સાયબર ક્રાઇમ હેલ્પલાઇન: જેમાં માંગેલ વિગતો ફોન પરજ આપવાની રહેશે.

સાયબર ક્રાઇમ
હેલ્પલાઇન નંબર
૧૯૩૦

જો આપની સાથે ઓનલાઇન નાણાંકિય ફ્રોડ કે અન્ય સાયબર ક્રાઇમ થાય છે તો તુરંત **૨૪ કલાક કાર્યરત** સાયબર ક્રાઇમ હેલ્પલાઇન નંબર ૧૯૩૦ પર કોલ કરો.

2. નેશનલ સાયબર ક્રાઇમ રીપોર્ટીંગ પોર્ટલ (NCCRP)

www.cybercrime.gov.in

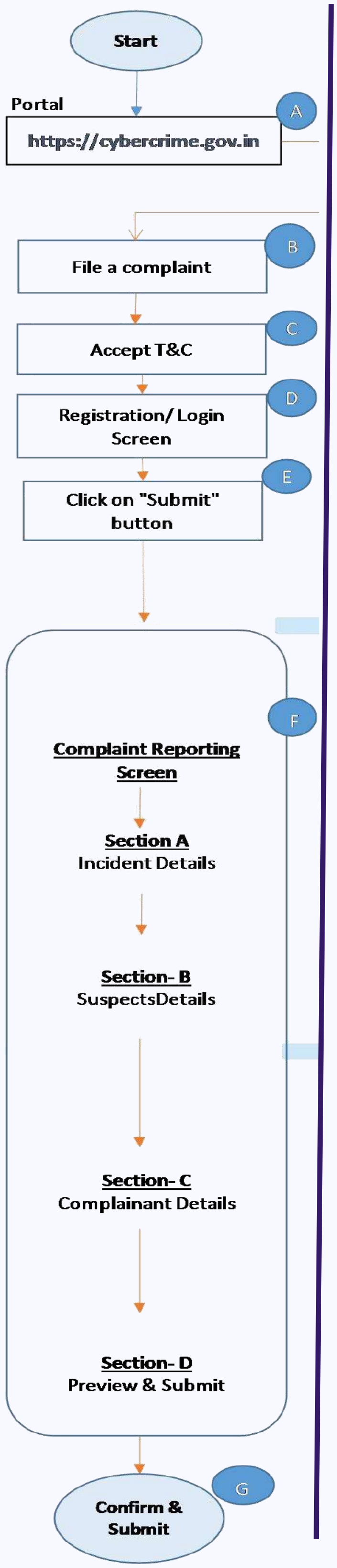
જો આપની સાથે સાયબર ક્રાઇમ થાય છે તો આપ નામી અથવા અનામી રીતે તમામ પ્રકારના સાયબર ક્રાઇમની ફરિયાદ ઓનલાઇન નેશનલ સાયબર ક્રાઇમ રીપોર્ટીંગ પોર્ટલ

NCCRP - www.cybercrime.gov.in

વેબસાઇટ પર કરી શકો છો.

સ્ટેટ સાયબર ક્રાઇમ સેલ દ્વારા તુરંત કાર્યવાહિ કરવામાં આવે છે

નેશનલ સાયબર ક્રાઇમ રીપોર્ટીંગ પોર્ટલ (NCCRP) પર ફરિયાદ નોંધાવવાની પ્રક્રિયા

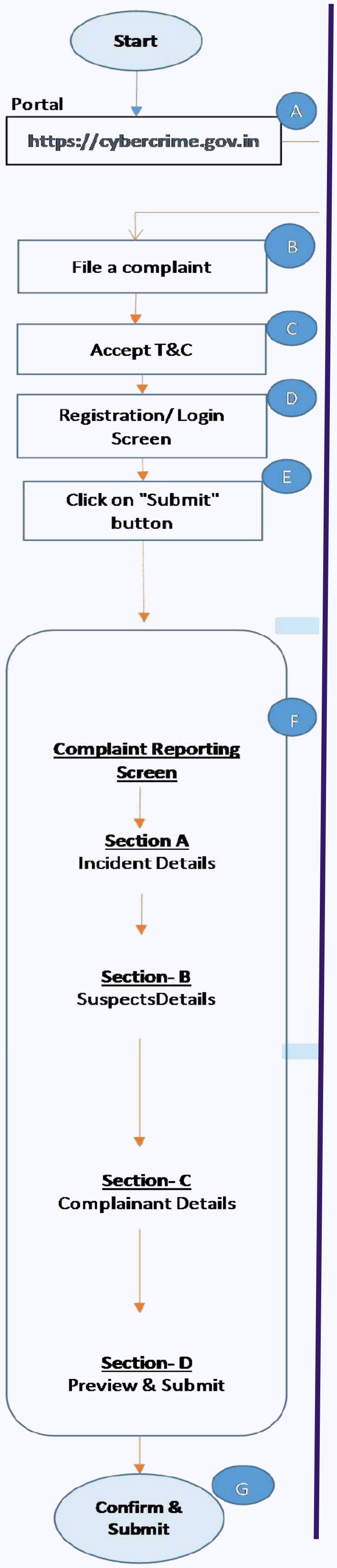


⇒ નેશનલ સાયબર ક્રાઇમ રીપોર્ટીંગ પોર્ટલ (NCCRP): www.cybercrime.gov.in ની મુલાકાત લો.

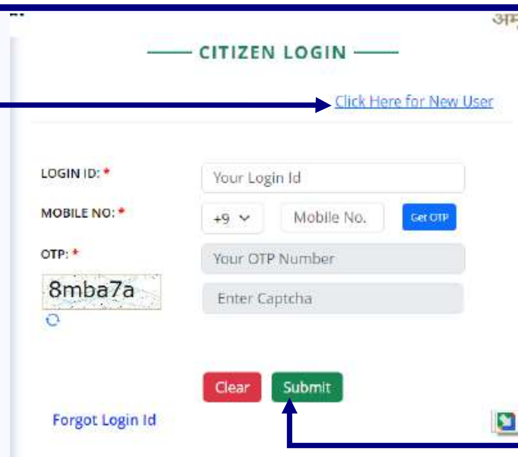
⇒ FINANCIAL FRAUD ટેબ પર Register a Complaint બટન પર ક્લિક કરો. ત્યાર બાદ નીચેની સ્ક્રીન ખુલશે જેમાંથી File a Complaint પર ક્લિક કરો.

⇒ ત્યાર બાદ privacy policy પેજ ખુલશે જેમાં I Accept બટન પર ક્લિક કરો. જેથી લોગીન પેજ ખુલશે

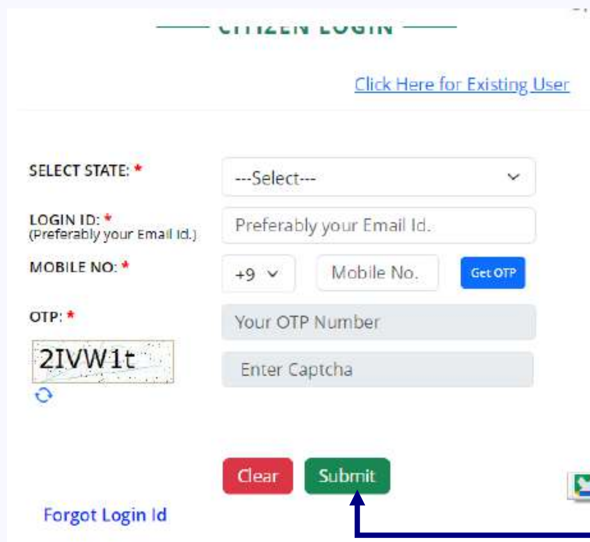
નેશનલ સાયબર ક્રાઇમ રીપોર્ટીંગ પોર્ટલ (NCCRP) પર ફરિયાદ નોધાવવાની પ્રક્રિયા



⇒ જો તમે પહેલા યુઝર આઈડી બનાવેલ હોય તો માંગેલ વિગતો ભરીને સબમિટ પર ક્લિક કરો. લોગીન પર ક્લિક કરો.

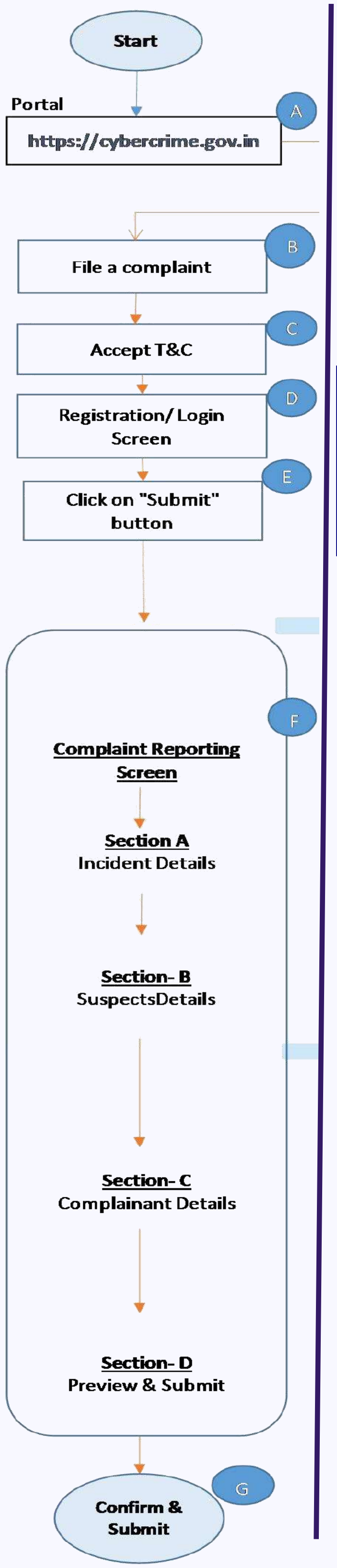


⇒ જો તમારી પાસે લોગીન આઈડી ન હોય તો નવું લોગીન આઈડી બનાવવા માટે Click Here for New User પર ક્લિક કરો.જેથી નીચની રજીસ્ટ્રેશન સ્ક્રીન ખુલશે જેમાં માંગ્યા મુજબ માહિતી ભરો જેથી તમારું રજીસ્ટ્રેશન થશે જેનો ઉપયોગ કરીને તમે લોગીન કરી શકશો.



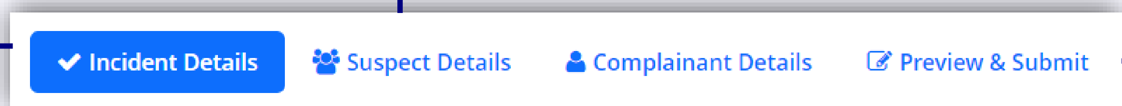
⇒ ત્યાર બાદ તમે લોગીન કરી શકશો.

નેશનલ સાયબર ક્રાઇમ રીપોર્ટીંગ પોર્ટલ (NCCRP) પર ફરિયાદ નોધાવવાની પ્રક્રિયા



⇒ વિભાગ A:– ઘટનાની વિગતો : જેમાં ઘટના કયા માધ્યમ પર બની તેની વિગતો તેમજ ઘટનાને લગતા પુરાવા અપલોડ કરવાના રહેશે. માંગ્યા મુજબ માહિતી આપ્યા બાદ NEXT બટન પર ક્લિક કરો.

⇒ વિભાગ B:– શંકાસ્પદ વિગતો : જેમાં શંકાશ્પદ નામ, તથા શંકાસ્પદ વ્યક્તિની વિગતો જો ઉપલબ્ધ હોયતો. માંગ્યા મુજબ માહિતી આપ્યા બાદ NEXT બટન પર ક્લિક કરો.



⇒ વિભાગ C: ફરિયાદી ની વિગતો : જેમાં નામ, માતા, પિતા વગેરે , આઇડી પ્રૂફ, અને જો તેમે બીજા વતી ફરિયાદ નોંધાવતા હોય તો તે વ્યક્તિ સાથે નો સબધ વગેરે મુજબ માહિતી આપ્યા બાદ NEXT બટન પર ક્લિક કરો.

⇒ વિભાગ D: પ્રિવ્યુ અને સબમિટ: ઉપરોક્ત ત્રણે ટેબ માં માંગ્યા મુજબ માહિતી ભર્યા બાદ તમારી અરજી દેખાશે જે ચકાશીને સબમિટ કરવાથી કન્ફર્મ થશે અને તમને અરજી નંબર સાથેની PDF મળશે.

⇒ આમ, ઉપરોક્ત તમામ સ્ટેપ્સ અનુસર્યા બાદ તમારી અરજી સાયબર સેલ ને મળી જશે અને સાયબર સેલ આ ફરિયાદ પર ત્વારિત કાર્ય શરુ કરશે. ઉપરાંત તમે આપણી કાલુપુર બેંક ના હેલ્પ ડેસ્ક નંબર: 079-27582020-26 પર કોલ કરી શકો છો.

સાયબર ક્રાઈમ સામે સલામતીની ટીપ્સ

સાયબર ક્રાઈમની બેંકમાં જાણ

જો આપની સાથે ઓનલાઈન નાણાંકીય ફ્રોડ કે અન્ય સાયબર ક્રાઈમ થાય તો તેની જાણ બેંકને કરવા માટે સંપર્ક કરો.

24X7 હેલ્પલાઈન નંબર

079-66215894 To 96

અથવા

ઈ-મેઈલ કરો

helpdesk@kalupurbank.com

તાત્કાલિક ધોરણે તમારું ડેબીટ કાર્ડ / UPI બ્લોક કરવા / એકાઉન્ટ ફ્રીઝ કરવા માટે તમારા રજીસ્ટર્ડ મોબાઈલ નંબર પરથી બેંક ના SMS મોબાઈલ નંબર **9028048500** પર નીચે મુજબ SMS કરો.

ડેબીટ કાર્ડ બ્લોક કરવા માટે :

BLOCK XXXX

(જ્યાં XXXX ની જગ્યાએ તમારા ડેબીટ કાર્ડ ના છેલ્લા 4 અંક એન્ટર કરવા)

UPI બ્લોક કરવા માટે :

UPI BLOCK XXXXXXXXXXX

(જ્યાં XXXXXXXXXXX ની જગ્યાએ તમારો ખાતા નંબર એન્ટર કરવો)

એકાઉન્ટ ફ્રીઝ કરવા માટે :

FREEZ XXXXXXXXXXX

(જ્યાં XXXXXXXXXXX ની જગ્યાએ તમારો ખાતા નંબર એન્ટર કરવો)

ગુજરાત રાજ્યમાં સ્થપાયેલ સાયબર ક્રાઇમ પોલીસ સ્ટેશન / સાયબર ક્રાઇમ સેલની યાદી અને સંપર્ક માહિતી.

અનુ.નં.	સાયબર ક્રાઇમ પોલીસ સ્ટેશન/સેલનું નામ	સંપર્ક નંબર	ઇ-મેઇલ એડ્રેસ
૧	સ્ટેટ સાયબર સેલ, સી.આઇ.ડી ક્રાઇમ, ગુજરાત રાજ્ય, ગાંધીનગર	૦૭૯-૨૩૨૫૦૭૯૮	cc-cid@gujarat.gov.in
૨	સાયબર ક્રાઇમ સેલ, અમદાવાદ શહેર	૦૭૯-૨૨૮૬૧૯૧૭	dcp-cybercrime-ahd@gujarat.gov.in
૩	સાયબર ક્રાઇમ સેલ, સુરત શહેર	૦૨૬૧-૨૬૫૩૫૧૦	acp-cyber-sur@gujarat.gov.in
૪	સાયબર ક્રાઇમ સેલ, વડોદરા શહેર	૦૨૬૫-૨૪૩૧૪૧૪	cp-cyber-vad@gujarat.gov.in
૫	સાયબર ક્રાઇમ સેલ, રાજકોટ શહેર	૦૨૮૧-૨૪૩૩૬૧૧	tp-raj@gujarat.gov.in
૬	સાયબર ક્રાઇમ પોલીસ સ્ટેશન, અમદાવાદ રેન્જ	૦૭૯-૨૯૭૦૫૪૭૦	cyber-range-ahd@gujarat.gov.in
૭	સાયબર ક્રાઇમ પોલીસ સ્ટેશન, સુરત રેન્જ	૦૨૬૧-૨૬૫૫૬૪૧	cyber-igp-sur@gujarat.gov.in
૮	સાયબર ક્રાઇમ પોલીસ સ્ટેશન, વડોદરા રેન્જ	૦૨૬૫-૨૪૧૦૦૪૬	cyber-crime-vr@gujarat.gov.in
૯	સાયબર ક્રાઇમ પોલીસ સ્ટેશન, રાજકોટ રેન્જ	૦૨૮૧-૨૪૭૪૨૧૫	cyber-igp-raj@gujarat.gov.in
૧૦	સાયબર ક્રાઇમ પોલીસ સ્ટેશન, ગાંધીનગર રેન્જ	૦૭૯-૨૩૨૬૦૬૧૫	cyber-gnr-range@gujarat.gov.in
૧૧	સાયબર ક્રાઇમ પોલીસ સ્ટેશન, ગોધરા રેન્જ	૦૨૬૭૨-૨૪૫૦૪૯	cyber-panch-range@gujarat.gov.in
૧૨	સાયબર ક્રાઇમ પોલીસ સ્ટેશન, જુનાગઢ રેન્જ	૦૨૮૫-૨૬૫૬૧૦૦	cybercrime-igp-jun@gujarat.gov.in
૧૩	સાયબર ક્રાઇમ પોલીસ સ્ટેશન, ભાવનગર રેન્જ	૦૨૭૮-૨૫૧૨૮૧૦	pi-ccc-bav@gujarat.gov.in
૧૪	સાયબર ક્રાઇમ પોલીસ સ્ટેશન, બોર્ડર રેન્જ	૦૨૮૩૨-૨૯૬૨૦૦	pi-polstn-ccbr@gujarat.gov.in
૧૫	સાયબર ક્રાઇમ પોલીસ સ્ટેશન, આણંદ	૦૨૬૯૨-૨૬૦૦૧૫	polstn-cybercrim-and@gujarat.gov.in
૧૬	સાયબર ક્રાઇમ પોલીસ સ્ટેશન, સાબરકાંઠા	૦૨૭૭૨-૨૪૭૩૩૩	cybercell-sp-sab@gujarat.gov.in
૧૭	સાયબર ક્રાઇમ પોલીસ સ્ટેશન, મહેસાણા	૦૨૭૬૨-૨૨૨૧૦૦	cybercell-meh@gujarat.gov.in
૧૮	સાયબર ક્રાઇમ પોલીસ સ્ટેશન, ભરૂચ	૦૨૬૬૪-૨૨૩૩૦૩	cybercrime-bha@gujarat.gov.in
૧૯	સાયબર ક્રાઇમ પોલીસ સ્ટેશન, વલસાડ	૦૨૬૩૨-૨૫૩૩૩૩	cyber-val@gujarat.gov.in
૨૦	સાયબર ક્રાઇમ પોલીસ સ્ટેશન, જામનગર	૦૨૮૮-૨૬૬૬૬૧૦	cybercell-sp-jam@gujarat.gov.in
૨૧	સાયબર ક્રાઇમ પોલીસ સ્ટેશન, પોરબંદર	૦૨૮૬-૨૨૪૦૦૮૦	cyberps-pbr@gujarat.gov.in
૨૨	સાયબર ક્રાઇમ પોલીસ સ્ટેશન, અમરેલી	૦૨૭૯૨-૨૨૩૪૯૮	cybercrime-sp-amr@gujarat.gov.in
૨૩	સાયબર ક્રાઇમ પોલીસ સ્ટેશન, કચ્છ-પશ્ચિમ (ભુજ)	૦૨૮૩૨-૨૫૮૦૨૯	uhc-cybercrime-bhuj@gujarat.gov.in
૨૪	સાયબર ક્રાઇમ પોલીસ સ્ટેશન, બનાસકાંઠા	૦૨૭૪૬-૨૫૩૬૪૦	cybercrime-pal-ban@gujarat.gov.in

કાલુપુર બેંક આપણી પોતાની બેંક

Head Office: "Kalupur Bank Bhavan"
Nr.Income Tax Circle, Ashram Road,
Ahemdabad-380014

Phone: 079-27582020 to 26
Email: info@kalupurbank.com
Website: www.kalupurbank.com