જા.ક્ર.:મા-૨/૨૦૨૪/ 13382

જિલ્લા શિક્ષણાધિકારી કચેરી,
એ-3, જિલ્લા સેવા સદન-૨,
અઠવાલાઈન્સ, સુરત,
તા.09/૦૯/૨૦૨૪.

પ્રતિ,

આચાર્યશ્રી,

પ્રાથમિક, માધ્યમિક અને ઉચ્ચત્તર માધ્યમિક શાળાઓ તમામ,

સુરત, જિ. સુરત.

વિષય : સાયબર ક્રાઈમ માહિતી પુસ્તિકા થી તમામ વિદ્યાર્થીઓને માહિતગાર કરવા બાબત.

ઉપરોક્ત વિષય અન્વયે જણાવવાનું કે આ સાથે સામેલ સાયબર ક્રાઈમ સેલ, સુરત શહેર દ્વારા પ્રકાશિત કરાયેલ "સાયબર ક્રાઈમ માહિતી પુસ્તિકા" થી તમામ વિદ્યાર્થીઓને સુમાહિતગાર કરવા જણાવવામાં આવે છે. જેથી આજના ડીજીટલ યુગમાં થતા સાયબર ક્રાઈમ અને તેના જુદા જુદા પ્રકાર વિષે વિદ્યાર્થીઓ અવગત થાય અને તેનાથી બચી શકે.

બિડાણ - સાયબર ક્રાઈમ માહિતી પુસ્તિકા

જિલ્લા શિક્ષણાધિકારી
સુરત, જિ-સુરત

#CyberSafeSurat

સાયબર સેફ સુરત

તમારી સાથે, તમારા માટે

આપણી સુરક્ષા
આપણા હાથમાં.

સાઇબર ક્રાઇમ માહિતી પુસ્તિકા

સાયબર ક્રાઇમ સેલ, સુરત શહેર

DIAL 1930
to report cyber crime

www.cybercrime.gov.in

#CyberSafeSurat

NEVER ACCEPT
DO NOT SHARE
Mobile Zone

1930

LACOSTE

CYBER SANJIVANI
CYBER CRIME CELL
• SURAT CITY •
आपकी सुरक्षा आपके हाथ में।

-:પ્રસ્તાવના:-

આજના ડિજિટલ યુગમાં, જ્યાં નેટવર્કના વિશાળ વેબ દ્વારા વિશ્વ એકબીજા સાથે જોડાયેલું છે, સાયબર જાગૃતિ હવે લક્ઝરી નહીં પરંતુ આવશ્યકતા છે. આપણું વ્યક્તિગત જીવન, વ્યાવસાયિક જવાબદારીઓ અને સામાજિક કાર્યો વધુને વધુ ડિજિટલ ટેકનોલોજીના સુરક્ષિત અને કાર્યક્ષમ ઉપયોગ પર આધારિત છે. જો કે, ટેક્નોલૉજી પરની આ નિર્ભરતા અંતર્ગત જોખમો સાથે આવે છે જે આપણી ગોપનીયતા, સુરક્ષા અને સુખાકારીને જોખમમાં મૂકે છે.

આ સાયબર અવેરનેસ બુકલેટ આપ સૌના ડિજિટલ લેન્ડસ્કેપને સુરક્ષિત અને જવાબદારી પૂર્વક નેવિગેટ કરવા માટે જ્ઞાન અને સાધનોથી સજ્જ કરવા માટે બનાવવામાં આવેલ છે. તેનો ઉદ્દેશ સાયબર જોખમોને ઓળખવા, સમજવા અને ઘટાડવા પર આવશ્યક માહિતી પ્રદાન કરીને સાયબર તકેદારીને પ્રોત્સાહન આપવાનો છે. આપના વ્યક્તિગત ડેટાને સુરક્ષિત કરવાના ફિશિંગ પ્રયત્નોની માહિતી આપવાથી લઈને, આ પુસ્તિકાનો દરેક વિભાગ સાયબર સલામતીના નિર્ણાયક પાસાઓને સંબોધિત કરે છે.

અમારું માનવું છે કે જાણકાર વ્યક્તિઓ સાયબર જોખમો સામે સંરક્ષણની પ્રથમ લાઇન છે. આપને આ જ્ઞાન સાથે સશક્ત બનાવીને અમે આપની ડિજિટલ સાક્ષરતામાં વધારો કરવાની અને એ સુનિશ્ચિત કરવાની આશા રાખીએ છીએ કે આપ સાયબર જોખમોથી જાતે, આપના પરિવારને અને આપની સંસ્થાનું રક્ષણ કરી શકો.

ચાલો આપણે સુરક્ષિત ડિજિટલ વિશ્વ તરફની આ યાત્રા શરૂ કરીએ, જ્યાં જાગૃતિ અને સક્રિય પગલાં આપણા સાયબર સંરક્ષણનો પાયો બની શકે અને સંયુક્તપણે આપણે “એક સાયબર સેફ સુરત શહેર” સમુદાયનું નિર્માણ કરીએ, જે સતત વિકસતા સાયબર ક્રાઈમના પડકારોનો સામનો કરી શકે.

છેલ્લા કેટલાક વર્ષોમા આપણો ભારત દેશ ઉત્તરોત્તર વિજ્ઞાન અને ટેક્નોલોજી ક્ષેત્રે પ્રગતિ કરી વિશ્વકક્ષાએ આગળ વધી રહ્યો છે. સાથે સાથે આ ડીજીટલ યુગમા ડીજીટલ બેંકિંગ અને સોશિયલ મિડીયાનો વ્યાપ ખૂબ વધ્યો છે. આ સાથે અપરાધિક માનસ ધરાવતા લોકોથી સતર્ક રહેવાની જરૂરીયાત ઉભી થઇ છે.જે માટે ગુજરાત સરકાર દ્વારા વિવિધ જાગૃતિના અભિયાન શરૂ કરવામા આવ્યા છે.

ભારત સરકારના NCCRP પોર્ટલ ૧૯૩૦ના માધ્યમથી નાગરિકોને ત્વરિત સહાય કરવા માટે ૨૪x૭ કાર્યરત સાયબર હેલ્પ લાઈન શરૂ કરવામાં આવેલ છે. આ સાથે રાજ્યના ૦૪ શહેરો, તમામ ૦૯ રેન્જ કચેરી તથા ૧૦ જિલ્લાઓમાં સાયબર ક્રાઇમ પોલીસ સ્ટેશન કાર્યરત કરવામા આવેલ છે.

સુરત શહેર પોલીસ દ્વારા હાથ ધરાયેલ ‘સાયબર સેફ સુરત’ અભિયાન હેઠળ આશરે ૨૦ લાખથી વધુ લોકોને જાગૃત કરવામાં આવ્યા છે. આ ઉપરાંત સુરત શહેરમાં સાયબર ક્રાઇમ અંગેની જાગૃતિ ફેલાવવા વિવિધ શાળા કોલેજોમા એક્સપર્ટ લેક્ચર તેમજ સેમિનાર યોજી યુવાઓને ‘જ્ઞાનની સાથે સતર્કતા’નો અનોખો અભિગમ સૂચવવામા આવ્યો. આ સાથે સુરત શહેર પોલીસ દ્વારા આ નવનિર્મિત ‘ સાયબર ક્રાઇમ માહિતી પુસ્તિકા’ દ્વારા દરેક વર્ગના લોકોને અનુલક્ષી આજના યુગના નવીનત્તમ સાયબર ક્રાઇમ વિશે તેમજ તેમાંથી સલામત રહેવાની વિસ્તૃત માહિતી આપવાનો પ્રયાસ કરેલ છે.

હું ગૃહ રાજ્યમંત્રી તરીકે આ ખૂબ ઉપયોગી અને સમજવામા સરળ એવી સાયબર ક્રાઇમ અંગેની માહિતી પુસ્તિકા પ્રકાશિત કરવા બદલ સુરત શહેર પોલીસ કમિશ્નરશ્રી તેમજ સાયબર ક્રાઇમ સેલ સુરત શહેરને અભિનંદન અને શુભેચ્છા પાઠવુ છું.

શ્રી હર્ષ સંઘવી
ગૃહ રાજ્યમંત્રી, ગુજરાત સરકાર

ગુજરાત પોલીસ રાજયના તમામ નાગરિકોની સેવા અને સુરક્ષા માટે હંમેશા કટિબધ્ધ રહે છે. લોકોને સુરક્ષા અને શાંતિની અનુભૂતિ કરાવી, લોકો પોતાનો સર્વાંગી વિકાસ કરી શકે તે માટે ગુજરાત પોલીસ તત્પર રહે છે. વિજ્ઞાન અને ટેકનોલોજીના આધુનિક યુગમાં ટેકનોલોજીના વિકાસની સાથે સાયબર ક્રાઇમ અને ગુનેગારોની મોડસ ઓપરેન્ડીમાં પણ ફેરફાર આવેલ છે. આ અનુલક્ષમાં પોલીસ પણ સાયબર ક્રાઇમ પોલીસ સ્ટેશનનાં માધ્યમથી સાયબર ગુનેગારોને ઝડપી પાડી સજા કરાવવા તત્પરતાથી કાર્યરત તો છે જ, સાથે સાથે લોકોમાં જાગૃતિ ફેલાવી, સાયબર ક્રાઇમને લગતા ગુનાઓ બનતા અટકાવવા માટે પણ કટિબધ્ધ છે.

સુરત શહેર પોલીસ દ્વારા પણ સાયબર સેફ સુરત જેવા જાગૃકતા મિશનને હાથ ધરી, મોટા પાયા પર લોકોમાં સાયબર સતર્કતા લાવવામાં આવી રહેલ છે. જેમાં વિવિધ નાટકો, માહિતી પુસ્તિકા, વિવિધ સેમીનાર જેવા અલગ અલગ માધ્યમથી આ માહિતી આપવામાં આવે છે.

આ ઉપરાંત સુરત શહેર પોલીસ દ્વારા સાયબર મિત્ર સુરત ચેટ બોટ નંબર- 9328523417 પર લોકોને "Ease of Access" મળી રહે છે, તેમજ સુરત શહેર સાયબર ક્રાઇમ દ્વારા હેલ્પ લાઇન નંબર મારફતે પણ સાયબર ક્રાઇમ લગત તેમજ તેની મોડસ ઓપરેન્ડી અને તેના બચાવ અંગેની માહિતી પૂરી પાડવામાં આવે છે.

આ પુસ્તિકામાં આપેલ ઉપયોગી માહિતી સામાન્ય માણસ સમજી શકે તેવી સરળ ભાષામાં પ્રકાશિત કરી, લોકોમાં સાયબર ક્રાઇમ સંદર્ભે વધુમાં વધુ જાગૃતિ લાવવા વિસ્તૃત સમજ આપવાનો પ્રયત્ન કરવામાં આવેલ છે તે બદલ હું સુરત શહેર પોલીસ કમિશ્નરશ્રી તેમજ સુરત શહેર સાયબર ક્રાઇમ સેલને અભિનંદન પાઠવું છું.

વિકાસ સહાય, IPS
પોલીસ મહાનિદેશક અને મુખ્ય પોલીસ અધિકારી,
હેડ ઓફ પોલીસ ફોર્સ, ગુજરાત રાજય, ગાંધીનગર.

પોલીસ કમિશનર તરીકે, હું આજે આપ સૌને આપણા ડિજિટલ ક્ષેત્રની સલામતીને લગતો એક મહત્વપૂર્ણ સંદેશ આપવા માંગુ છુ.આપણે એવા યુગમાં છીએ જ્યાં ટેકનોલોજી આપણા જીવનના દરેક પાસામાં વ્યાપ્ત છે, ત્યારે સાયબર ક્રાઇમના તોળાઇ રહેલા ખતરા સામે આપણે સતર્ક રહેવું અનિવાર્ય છે.

સાયબર ક્રાઇમને કોઈ સીમાડા નથી. તે ગમે ત્યાં, કોઈપણ સમયે કોઈની સાથે પણ થઈ શકે છે. ફિશિંગ ટેકનિકથી માંડીને, ડેટા બ્રિચ સુધી, સાયબર ગુનેગારો આપણી નબળાઈઓનો લાભ લેવા માટે અવનવી યુક્તિઓ સતત વિકસિત કરી રહ્યા છે. આ માત્ર આપણી વ્યક્તિગત માહિતી અને નાણાકીય અસ્કયામતોને જ જોખમમાં નથી મુકતા, પરંતુ આપણા સમાજને એક જુટ રાખનાર વિશ્વાસને પણ નબળા પાડે છે.

સાયબર ગુનાની પ્રતિક્રિયાઓ ડિજિટલ ક્ષેત્રથી ઘણી આગળ વિસ્તરે છે. તે ધંધાઓને બરબાદ કરી શકે છે, મહત્ત્વપૂર્ણ માળખાગત સુવિધાઓને વિક્ષેપિત કરી શકે છે અને જીવનને પણ જોખમમાં મૂકી શકે છે. એટલે જ, આ જોખમનો સામનો કરવા માટે આપણા સામૂહિક પ્રયાસની જરૂર છે.

જાગૃતિ એ સાયબર જોખમો સામે સંરક્ષણની પ્રથમ લાઇન છે. સાયબર કૌભાંડો વિશે આપણી જાતને શિક્ષિત કરી, સાયબર સ્વચ્છતાની પ્રેક્ટિસ જાળવીને અને સુરક્ષા ટીપ્સથી વાકેફ રહીને, આપણે સાયબર હુમલાઓને નોંધપાત્ર રીતે ઘટાડી શકીએ છીએ.

પોલીસ કમિશનર તરીકે, હું આપ સૌને ખાતરી આપું છું કે સુરત શહેર પોલીસ સાયબર ગુનાઓને ડામવા માટે પ્રતિબદ્ધ છે. અમે અમારી ક્ષમતાઓને સતત વધારી રહ્યા છીએ અને અત્યાધુનિક ટેકનોલોજીનો ઉપયોગ કરી રહ્યા છીએ, જેથી આ સતત વિકસી રહેલાં સાયબર ક્રાઇમના ગુનાઓનો સામનો કરી શકાય.

જ્યારે સાયબર ક્રાઇમની વાત આવે છે, ત્યારે જાગૃતિએ આપણું સૌથી મજબૂત શસ્ત્ર છે. જેથી આ પુસ્તિકામાં આપેલ માહિતી દ્વારા નાગરિકો સાયબર ગુનાઓની અલગ અલગ મોડસ ઓપરેન્ડી વિષે તથા સાયબર ગુનાઓના નિવારણ માટે કેવી સાવચેતી રાખવી તે વિષે અવશ્ય માહિતગાર થશે.

"સુરક્ષિત રહો, સતર્ક રહો"

શ્રી અનુપમ સિંગ ગહલૌત, IPS
પોલીસ કમિશ્નર, સુરત શહેર

આજના ઝડપથી વિકસતા ડિજિટલ યુગમાં, આપણી દૈનિક પ્રવૃત્તિઓ માટે આપણે ઇન્ટરનેટ પર વધુમાં વધુ નિર્ભર થઇ ગયેલ છીએ. ઇન્ટરનેટના ઉપયોગ કરવાના ફાયદા અને ગેરફાયદા બંને છે. દરરોજ અલગ અલગ પધ્ધતિથી સાયબર ગુનાઓ નોંધાય છે. ગુજરાત સરકાર સાયબર ક્રાઇમના ગુનાઓ રોકવા સંપુર્ણ રીતે પ્રયત્નશીલ છે, પરંતુ સાયબર ગુનાઓથી સલામત રહેવા માટે સાવચેતી રાખવી આપણી પણ ફરજ છે. એક હકીકત છે કે, જો આપણે વિવિધ સાયબર ક્રાઇમના પ્રકાર વિષે જાગૃત હોઇએ તો પોતાને, પોતાના પરિવારને તથા મિત્રોને સાયબર ગુનાઓથી સુરક્ષિત રાખી શકીએ. જેથી સાયબર ગુનાઓથી નાગરિકોને સુરક્ષિત રાખવા તથા મહિલાઓ અને બાળકો પણ ઇન્ટરનેટ ઉપર સલામત રહે તે ઉદ્દેશથી સુરત શહેર પોલીસ દ્વારા વિવિધ અવેરનેસ કાર્યક્રમોના માધ્યમથી નાગરિકોને સુરક્ષિત રાખવાની પહેલ કરવામાં આવેલ છે.

મને એ જણાવતા આનંદ થાય છે કે, સાયબર ક્રાઈમ સેલ, સુરત શહેર દ્વારા "સાયબર ક્રાઈમ નિવારણ અને જાગૃતિ" માટેની આ પુસ્તિકા તૈયાર કરવામાં આવેલ છે. આ પુસ્તિકામાં સાયબર સુરક્ષા સંબંધી આપેલ ટીપ્સ તથા માહિતીથી આપને રોજબરોજના થતા સાયબર ગુનાઓ/છેતરપિંડીથી સુરક્ષિત રહેવામાં અવશ્ય મદદ મળશે. હું સુરત શહેરને સાયબર ગુનાઓથી સલામત રાખી "સાયબર સેફ" સુરત શહેર બનાવવાના સાયબર ક્રાઈમ સેલ, સુરત શહેરના પ્રયાસને બિરદાવું છું અને શુભેચ્છા પાઠવું છું.

શ્રી રાઘવેન્દ્ર વત્સ, IPS
સંયુક્ત પોલીસ કમિશ્નર (ક્રાઇમ),
સુરત શહેર

Index

૧. સાયબર ક્રાઈમ શું છે?..૦૯
૨. ડિજિટલ એરેસ્ટ ફ્રોડ...૧૦
3. AI (Artificial Intelligence) વૉઈસ ક્લૉનીંગ ફ્રોડ.........૧૩
૪. ડીપફેક વિડીયો કોલ ફ્રોડ...૧૪
૫. ઓનલાઈન ટાસ્ક ફ્રોડ..૧૫
૬. ઇન્વેસ્ટમેન્ટ ફ્રોડ (ફોરેક્સ /શેર ટ્રેડિંગ)..........................૧૬
૭. મોર્ફ્ડ ફોટો/ન્યુડ વિડિયો કોલ ફ્રોડ (Sextortion)..........૧૮
૮. ફેક લોભામણી જાહેરાતો..૧૯
૯. OTP/CVV/PIN નંબર મેળવી થતા ફ્રોડ..........................૨૦
૧૦. ગુગલ કસ્ટમર કેર નંબર સર્ચ ફ્રોડ..................................૨૧
૧૧. ઈન્સ્ટન્ટ લોન એપ્લિકેશન ફ્રોડ.......................................૨૨
૧૨. ક્રિપ્ટો કરન્સી ફ્રોડ..૨૩
૧૩. ઇલેક્ટ્રીસીટી બીલ ફ્રોડ..૨૪
૧૪. મેટ્રીમોનીયલ ફ્રોડ..૨૫
૧૫. લોન ફ્રોડ...૨૬
૧૬. ઈન્સ્યોરન્સ ફ્રોડ...૨૭
૧૭. જોબફ્રોડ..૨૮
૧૮. લોટરી ફ્રોડ..૨૯
૧૯. OLX ફ્રોડ...30
૨૦. પોન્ઝી સ્કીમ ફ્રોડ...3૧
૨૧. સીમ સ્વેપિંગ ફ્રોડ...3૨
૨૨. ઇન્કમટેક્ષ રીફંડ ફ્રોડ..33
૨3. ઓનલાઇન ગેમિંગ ફ્રોડ..33
૨૪. ફ્રેન્ડશીપ ક્લબ ફ્રોડ..3૫
૨૫. OTP આપ્યા વગર થતા ફ્રોડ: (કાર્ડ ક્લૉનિંગ)...................3૬
૨૬. સાયબર બુલિંગ..3૭
૨૭. સાયબર સ્ટોકિંગ..3૮
૨૮. આઇડેન્ટીટી થેફ્ટ..3૯
૨૯. ઈ-મેઈલ ફિશિંગ..૪૦
30. રેન્સમવેર...૪૧
3૧. પ્રાઈવસી સેટિંગ..૪૨
3૨. સોશિયલ મીડિયા ક્રાઈમથી બચવા માટેની ટીપ્સ............૪૪
33. નાણાકીય છેતરપિંડીથી બચવા માટેની ટીપ્સ...................૪૫
3૪. સાયબર સેલની સિદ્ધીઓ..૪૬
3૫. સાયબર ક્વિઝ..૫૨
3૬. સેલ્ફ રિપોર્ટીંગ પોર્ટલ..૫૬
3૭. સાયબર પ્રતિજ્ઞા...૬૧

સાયબર ક્રાઈમ શું છે?

સાયબર ગુનાઓ નાણાકીય અથવા બિન-નાણાકીય લાભ માટે ડિજિટલ માધ્યમથી કરવામાં આવતા અત્યાધુનિક ગુનાઓ છે. સરળ ભાષામાં, તેને કોઈપણ પ્રકારની લાલચ, છેતરપિંડી અથવા અન્ય વ્યક્તિઓને ઓનલાઈન હેરાનગતિને પ્રોત્સાહન આપવા માટે મોબાઈલ ફોન, કમ્પ્યુટર, લેપટોપ અને/અથવા ઈન્ટરનેટનો ઉપયોગ કરીને કોઈપણ ગેરવર્તણૂક તરીકે વ્યાખ્યાયિત કરી શકાય છે. તેમાં નાણાકીય છેતરપિંડી, અપમાનજનક ભાષાનો ઉપયોગ, પાસવર્ડ અથવા ડિજિટલ ડેટાની ચોરીનો સમાવેશ થાય છે.

સાયબર ક્રાઈમના પ્રકાર:

1) સોશિયલ મીડિયા સંબંધિત ફ્રોડ
2) નાણાકીય અથવા બેંકીંગ સંબંધિત ફ્રોડ
3) સાયબર ટેરેરિઝમ

નાણાકીય અથવા બેંકીંગ સંબંધિત ફ્રોડ

ડિજિટલ એરેસ્ટ ફ્રોડ

પાર્સલ એમ.ઓ. :સાયબર ક્રિમિનલ્સ C B I અધિકારી, કસ્ટમ અધિકારી અથવા પોલીસ અધિકારીનો સ્વાંગ રચી લોકોને વિડિયો અથવા ઓડિયો કોલ કરે છે અને જણાવે છે કે તેમણે કોઈ પાર્સલ વિદેશ મોકલ્યું છે અથવા વિદેશથી મેળવેલ છે, જેમાં ગેરકાયદે માલસામાન, ડ્રગ્સ, નકલી પાસપોર્ટ અથવા કોઈ પ્રતિબંધિત ચીજવસ્તુ છે. આવા કિસ્સાઓમાં ભોગ બનનારને સ્કાઇપ અથવા અન્ય વિડિયો કોન્ફરન્સિંગ પ્લેટફોર્મ પર હાજર રહેવા મજબૂર કરી તેઓને પોતાના ઘરમાં ડિજિટલી અરેસ્ટ થવાનું જણાવી બહારની દુનિયા સાથે સંપર્ક તોડાવી સમાધાન અને કેસ બંધ કરવા માટે પૈસાની માંગ કરે છે.
આવા કિસ્સાઓમાં ભોગ બનનાર લોકો ગભરાઈને કેસ પતાવવાનો પ્રયાસ કરે છે અને નાણા ચૂકવે છે

ગુનાહિત કૃત્ય એમ.ઓ. :સાયબર ક્રિમિનલ્સ પોલીસ અધિકારીનો સ્વાંગ રચી કેટલાક કિસ્સામાં ગુનેગારો ભોગ બનનારને સંપર્ક કરીને કહે છે કે તેમના પ્રિયજનો કોઈ છેડતી અથવા રેપ કેસમાં સંડોવાયેલા છે અને તેમની કસ્ટડીમાં છે. તેમજ એરેસ્ટ વોરંટ નીકળ્યુ છે તેવુ પ્રતીત કરાવે છે અને જ્યાં સુધી તેમની માંગણીઓ પૂરી ન થાય ત્યાં સુધી સ્કાઇપ અથવા અન્ય વિડિયો કોન્ફરન્સિંગ પ્લેટફોર્મ પર હાજર રહેવાની ફરજ પાડી ડિજિટલી એરેસ્ટ કરવામાં આવે છે.
સાયબર ગુનેગારો પોલીસ સ્ટેશન અથવા સરકારી કચેરીઓ જેવા દેખાતા સ્ટુડિયોનો ઉપયોગ, કાયદા અમલીકરણ એજન્સીઓ જેવા જ ગણવેશ, વોટ્સએપ ડી.પી.માં પોલીસ અધિકારીના ફોટા તથા કાયદા અમલીકરણ એજન્સી જેવા જ ખોટા એકાઉન્ટનો ઉપયોગ કરી વાસ્તવિકતા ઉપજાવી કાઢવા માટે જાણીતા છે. આવા કિસ્સાઓમાં ગુનેગારો સમાધાન અને કેસ બંધ કરવા માટે પૈસાની માંગ કરે છે. ભોગ બનનાર લોકો ગભરાઈને કેસ પતાવવાનો પ્રયાસ કરે છે અને નાણા ચૂકવે છે.

- પોલીસ અધિકારી કે કોઈ સરકારી અધિકારી વિડિયો/ઓડિયો કોલના માધ્યમથી કે skype અથવા અન્ય વિડિયો કોન્ફરન્સિંગ એપ્લીકેશન ડાઉનલોડ કરાવી ગુનેગારોને ડિજીટલી અરેસ્ટ કરતી નથી અથવા પુછપરછ કરતી નથી કે દંડરૂપે નાણાની માંગણી પણ કરતી નથી.
- પોલીસ અધિકારીના સ્વાંગમાં કોઈ અરેસ્ટ વોરંટ અથવા અન્ય ડોક્યુમેન્ટ ઓનલાઈન રજુ કરે તેને સાચી માની વ્યક્તિગત માહિતી અથવા તો ખાસ કરીને તમારી બેંકિંગ વિગતો ક્યારેય શેર કરશો નહીં. કે તેઓના દ્વારા આપવામાં આવતા એકાઉન્ટમાં નાણા ટ્રાન્સફર કરશો નહિ.
- કોઈપણ પગલું લેતા પહેલા ગભરાયા વગર નજીકના પોલીસ સ્ટેશન અથવા આપના પરિજનોનો સંપર્ક કરો.

ટેલિકોમ રેગ્યુલેટરી ઓથોરિટી ઓફ ઇન્ડિયાના નામે છેતરપિંડી

ભોગ બનનારને રેકોર્ડ કરેલા કોલ સાથે મોબાઇલ નંબરથી સંપર્ક કરવામાં આવે છે કે આ કોલ ટેલિકોમ રેગ્યુલેટરી ઓથોરિટી ઓફ ઇન્ડિયા તરફથી છે અને ર કલાકની અંદર તમારો મોબાઇલ નંબર બંધ થઇ જશે.

ટેલિકોમ રેગ્યુલેટરી ઓથોરિટી ઓફ ઇન્ડિયા(TRAI)ના સ્વાંગમાં સાયબર છેતરપિંડી કરનારાઓ દ્વારા ફોન કરી ભોગ બનનારને કહેવામાં આવે છે કે તેમના નામ, મોબાઇલ નંબર અથવા આધાર ઉપર સિમકાર્ડ મેળવવામાં આવેલ છે જેનો ઉપયોગ રાષ્ટ્ર વિરોધી પ્રવૃત્તિઓ, છેતરપિંડી અને સતામણી માટે કરવામાં આવી રહ્યો છે. જેના માટે તેઓ વિરુદ્ધ એફઆઇઆર નોંધવામાં આવી છે અને તેઓને ડરવવા કેટલાક બનાવટી એફઆઇઆરના નંબરો પણ શેર કરવામાં છે.

છેતરપિંડી કરનારાઓ ભોગ બનનારને ૯ નંબર ડાયલ કરવા કહે છે અને પછી સ્કાઇપ દ્વારા વીડિયો કોલ પર જોડાવા માટે દબાણ કરે છે, જ્યાં યુનિફોર્મમાં એક નકલી પોલીસ ફરિયાદીના નામ, સરનામાં અને અન્ય વિગતો સાથે બનાવટી એફઆઇઆરની વિગતો વાંચી સંભવળાવે છે. ધરપકડ ટાળવા માટે ભોગ બનનારને પોતાના ઘરમાં ડિજિટલી અરેસ્ટ થવાનું જણાવી બહારની દુનિયા સાથે સંપર્ક તોડાવી સમાધાન અને કેસ બંધ કરવા માટે પૈસાની માંગ કરે છે. આ રીતે સાયબર ફ્રોડસ્ટર છેતરપિંડી આચરી રહ્યા છે.

- તમારા આધારકાર્ડ અથવા મોબાઇલ નંબરનો દુરૂપયોગ કરવામાં આવ્યો છે તે અંગેના કોલ કરનારાઓ પર વિશ્વાસ કરશો નહીં
- ધરપકડના ડર હેઠળ કોઈપણ નાણાકીય અથવા અન્ય માંગણી કરે તો સાવચેત રહો અને કોઇ પણ નાણાં ચૂકવશો નહિ.
- છેતરપિંડી કરનારાઓના કોલ્સ રેકોર્ડ કરો અને સ્ક્રીન શોટ લેવાનું રાખો.
- સંચારસાથી પોર્ટલ (www.sancharsaathi.gov.in/sfc/) ઉપર ફ્રોડ નંબરો
- બ્લોક કરવા રિપોર્ટ કરો.

જો તમારી સાથે નાણાકીય છેતપિંડી થાય તો તાત્કાલિક સાયબર ક્રાઇમ પોલીસ અથવા ડાયલ 1930 નો સંપર્ક કરો અથવા www.cybercrime.gov.in પર લૉગ ઇન કરી આપની ફરિયાદ નોંધાવો.

AI (Artificial Intelligence) વોઈસ ક્લોનીંગ ફ્રોડ

સાયબર ફ્રોડસ્ટર હવે અવાજોને ક્લોન કરવા માટે AI નો ઉપયોગ કરી રહ્યા છે. આ પ્રકારના ફ્રોડ અંતર્ગત આર્ટિફિશિયલ ઈન્ટેલિજન્સનો ઉપયોગ કરીને હવે સાયબર છેતરપિંડી થઈ રહી છે. AIની મદદથી મિત્રો અને સંબંધીઓ જેવો જ અવાજ કાઢી ફોન કરીને પ્રિયજનો/મિત્રો સંકટમાં હોય તાત્કાલિક નાણાકીય મદદની જરૂર હોય તેવી રીત આજીજી કરતા સ્વરે વાત કરે છે અને મદદ માટે ઝડપથી મોટી રકમ ટ્રાન્સફર કરવાનું કહી છેતરપિંડી કરવામાં આવે છે.

- આવા પ્રકારના ફ્રોડ કોલ્સ આવે તો સાવચેત રહો આપના મિત્રો/પરિજનોનો પુન: સંપર્ક કરી ચકાસણી કરો.
- ઉતાવળમાં કોઈ નાણા ચુકવશો નહીં.
- આપને વારંવાર કોલ્સ આવે તો સાયબર ક્રાઈમ હેલ્પ લાઈનનો સંપર્ક કરો.

ડીપફેક વિડીયો કોલ ફ્રોડ

AI વોઈસ સ્કેમની જેમ વિડિયો કોલ દ્વારા પણ સ્કેમ થઈ રહ્યા છે. જેમા ગુનેગારો સોશ્યલ મીડિયા પર ઉપલબ્ધ ફોટા, વિડિયોનો ડીપફેક અને આર્ટિફિશિયલ ઈન્ટેલિજન્સના ઉપયોગથી કોઈના પરિચિત બનીને વિડિયો કોલ કરે છે અને કોઈને કોઈ બહાનુ બતાવીને પૈસા પડાવે છે. ઘણી વખત ડીપફેકનો ઉપયોગ કરીને અશ્લીલ તસવીરો અથવા વિડિયો બનાવીને લોકોને બ્લેકમેલ કરીને પણ લાખો રુપિયા પડાવે છે.

- આવા પ્રકારના ફ્રોડ કોલ્સ આવે તો સાવચેત રહો આપના મિત્રો/પરિજનોનો પુન: સંપર્ક કરી ચકાસણી કરો.
- આ પ્રકારના ફ્રોડથી બચવા માટે અજાણ્યા નંબરથી વિડિયો કોલ્સ આવે તો કોઈ પ્રતિભાવ આપશો નહીં.
- સાવચેત રહો ગભરાઈને કોઇ નાણા ચુકવશો નહીં.
- શરમ અને સંકોચ રાખ્યા વગર તરત પોલીસનો સંપર્ક કરો.

ઓનલાઈન ટાસ્ક ફ્રોડ

ટેલીગ્રામ/ઈન્સ્ટાગ્રામ/SMS/Whatsapp દ્વારા ઘરે બેઠા કમાવવા માટેના મેસેજ મોકલવામાં આવે છે. ઓનલાઇન ટાસ્ક (રીવ્યુ/ લાઇક્સ) પુરા કરવાથી પ્લાન મુજબ વળતર મળશે તેમ જણાવવામાં આવે છે. શરૂઆતમાં ઓછી રકમના પ્લાનમાં ટાસ્ક પુરા કરવાથી વળતર આપવામાં આવે છે. ત્યારબાદ પ્રિમિયમ/વી.આઈ.પી. પ્લાનમાં એડ થવાથી વધુ વળતર મળશે તેવું જણાવવામાં આવે છે. પ્રિમિયમ/ વી.આઈ.પી. પ્લાન લીધા બાદ ટાસ્ક પુરો કરતા સમયે નવા ઓર્ડર જનરેટ કરી નાણા પડાવવામાં આવે છે અને છેતરપિંડી કરવામાં આવે છે.

- આ પ્રકારના ફ્રોડથી બચવા માટે અજાણ્યા વ્યક્તિ દ્વારા અજાણી એપ્લીકેશન ડાઉનલોડ કરવા જણાવે તો એપ્લીકેશન ડાઉનલોડ કરશો નહીં.
- SMS/ઇ-મેઇલ દ્વારા મોકલવામાં આવેલ અજાણી શંકાસ્પદ લીંક પર ક્લીક કરશો નહીં. ઓનલાઇન ટાસ્ક કમ્પ્લીટ કરવાનું જણાવી ઉચ્ચ વળતર આપવામાં આવશે તેવી ભ્રામક જાહેરાતોથી સાવચેત રહેવું.
- સોશિયલ મિડીયા પ્લેટફોર્મ ઉપર આવતી લોભામણી ઓફરોથી લલચાશો નહીં.

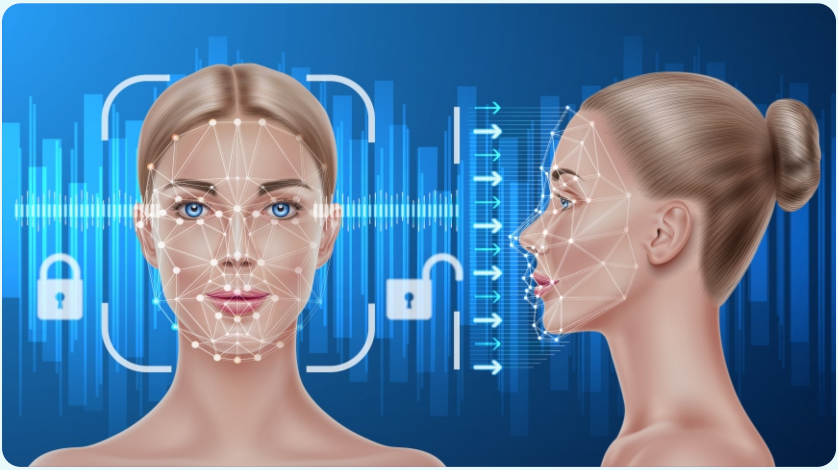
ફોરેક્સ /શેર ટ્રેડિંગ ફ્રોડ:

આ પ્રકારના ફ્રોડમાં ભોગ બનનારને છેતરપીંડી કરનાર લોકો દ્વારા ફોનથી કે વોટ્સએપ મેસેજથી સંપર્ક કરી ફોરેક્સ એક્ષચેન્જ/શેર માર્કેટમાં રોકાણ કરવાથી ઓછા સમયમાં તેઓના રોકાણમાં ખુબ સારો નફો મળી શકે છે, તેવું જણાવી તેઓના ફેક ટ્રેડિંગ એકાઉન્ટ બનાવી ખોટો નફો બતાવી મોટી રકમ રોકાણ કરવા લલચાવી છેતરપિંડી કરવામાં આવે છે. ઘણી બખત ભોગ બનનારને વોટ્સએપ, ટેલિગ્રામમાં અજાણ્યા નંબરો દ્વારા રોકાણ માટેનાં ગૃપમાં જોડી દેવામાં આવે છે.

- જો તમોને ફોરેક્સ/શેર ટ્રેડીંગના આવા કોઇ મેસેજ આવે તો તેનો કોઇ પ્રતિભાવ આપવો નહીં.
- અજાણ્યા નંબરથી વોટ્સએપ/ટેલીગ્રામ ગૃપમાં એડ કરવામાં આવે તો ગૃપમાંથી લેફ્ટ થઇ અજાણ્યા નંબરને બ્લોક કરો.
- લોભ, લાલચમાં આવી શરૂઆતમાં નાની રકમ નફામાં મેળવવા છતાં વિશ્વાસમાં આવી મોટું રોકાણ કરવું નહીં.
- ફેસબુક, ઈન્સટાગ્રામ, વોટ્સએપ જેવા સોશ્યલ મીડિયા પ્લેટફોર્મ પરથી લીંક દ્વારા ઈન્વેસ્ટમેન્ટની એપ્લિકેશન ડાઉનલોટ કરવાનું ટાળો

ફોટો મોર્ફીંગ

આ પ્રકારના ગુનામાં ભોગ બનનારના વિવિધ સોશિયલ મીડિયા પ્લેટફોર્મ પર અથવા અન્ય કોઇ રીતે મુકેલા ફોટાનો ઉપયોગ કરીને તેમાં એડીટીંગ કરી બિભસ્ત ફોટો બનાવી ભોગ બનનારને બદનામ કરવા, બ્લેકમેઇલ કરવા અથવા ડરાવવામાં આવે છે.



- સોશિયલ મીડિયા પ્રોફાઇલ પ્રાઇવેટ અને લોક રાખો.
- તમારા અંગત ફોટા ઓનલાઇન અપલોડ કરશો નહીં.
- અજાણ્યા લોકોની ફ્રેન્ડ રીક્વેસ્ટ સ્વીકારશો નહી.
- તમારા ફોનમાં ડાઉનલોડ કરેલ બધી એપ્લિકેશન્સને ફોન ગેલેરીનો એક્સેસ આપવો નહિ.

વીડિયો કોલ ફ્રોડ (Sextortion):

ફ્રોડ કરનાર વ્યક્તિ દ્વારા આપને સોશિયલ મીડિયા ઉપર સુંદર યુવતીના ફોટા વાળી પ્રોફાઇલથી ફ્રેન્ડ રીક્વેસ્ટ મોકલવામાં આવે છે. ફ્રેન્ડ રીક્વેસ્ટ સ્વીકાર્યા બાદ તેઓ તમારી સાથે ઘનિષ્ઠ સંબંધો કેળવી વોટ્સએપ નંબર મેળવી લે છે. ત્યારબાદ વીડિયો કોલ કરી આપને અભદ્ર ક્રિયા કરવા જણાવે છે અને સ્ક્રીનનું રેકોર્ડીંગ કરી આપનો વીડિયો યુ-ટ્યુબ ઉપર વાઇરલ કરવાની ધમકી આપે છે અને નાણાની માંગણી કરવામાં આવે છે. ઘણા કિસ્સામાં ક્રાઇમ બ્રાંચમાંથી/યુ ટ્યુબ માંથી બોલું છું તેવા કોલ પણ આવે છે.

- અજાણ્યા લોકોની ફ્રેન્ડ રીક્વેસ્ટ સ્વીકારવી નહીં.
- જો તમારી સાથે આવું કંઇ થાયતો તેઓ તમારો સંપર્ક કરી શકે નહીં તે માટે થોડો સમય આપનું વોટ્સ-એપ તથા સોશીયલ મીડિયા એકાઉન્ટ બંધ રાખવું.
- ધમકી આપવામાં આવે તો ગભરાઇને કોઇ નાણા ચુકવશો નહીં. શરમ અને સંકોચ રાખ્યા વગર તુરંત પોલીસનો સંપર્ક કરો.
- આવા ફ્રોડમાં એક વાર નાણા ચુકવવામાં આવે તો પણપણ અવારનાવર નાણાની માંગણી કરવામાં આવે છે.

ફેક લોભામણી જાહેરાતો:

સોશિયલ મીડિયા પ્લેટફોર્મ ઉપર જુદી જુદી પ્રખ્યાત કંપની, હોસ્પિટલ તથા રેસ્ટોરન્ટના નામે લોભામણી અને લલચામણી ફેક જાહેરાત બનાવી મુકવામાં આવે છે. નાગરિકો દ્વારા જાહેરાતમાં આપેલ લીંક ઉપર ક્લિક કરવાથી અથવા આપેલ ફોન નંબર ઉપર સંપર્ક કરવાથી તેઓના બેંક એકાઉન્ટની માહિતી મેળવી નાંણાકીય છેતરપીંડી કરવામાં આવે છે અથવા હલકી ગુણવત્તાની સાધનસામગ્રી મળે છે અથવા મળતી જ નથી.

- સોશિયલ મીડિયા પ્લેટફોર્મ ઉપર મુકવામાં આવેલ લોભામણી જાહેરાતથી લલચાશો નહીં.
- હંમેશા કોઇપણ ઓનલાઇન ખરીદી વિશ્વાસુ અને પ્રમાણિત વેબસાઇટ ઉપરથી કરો.

OTP/CVV/PIN નંબર મેળવી થતા ફ્રોડ:

નાગરીકોને ફોન દ્વારા બેંક મેનેજર કે બેંક કર્મચારી તરીકેની ઓળખ આપી KYC અપડેટ કરવા, ક્રેડિટ કાર્ડ માં લીમીટ વધારવા માટે, ક્રેડિટ કાર્ડ એક્ટીવેટ કરવા માટે, બેંક એકાઉન્ટ બંધ થઇ જશે તેવા અલગ-અલગ રીતે લાલચ, ભય કે ખોટી માહિતી આપીને વિશ્વાસ કેળવીને નાગરીકોની ડેબિટ કાર્ડ/ ક્રેડિટ કાર્ડ સંબંધી માહિતી અને OTP/CVV/PIN નંબર મેળવી અથવા તો Anydesk, Quick Support, Team Viewer જેવી સ્ક્રીન શેરીંગ એપ્લિકેશન ડાઉનલોડ કરાવી છેતરપીંડી કરવામાં આવે છે.

- બેંક કર્મચારીઓ ફોન કરીને એકાઉન્ટ ધારકના OTP/CVV/PIN માંગતા નથી.
- KYC ઓનલાઇન અપડેટ કરવામાં આવતું નથી. જેથી આ માટે રૂબરૂ સંબંધિત ઓફિસનો સંપર્ક કરવો.
- કોઇપણને OTP/CVV/PIN નંબર આપવો નહીં.
- અજાણ્યા દ્વારા મોકલવામાં આવેલ લીંક અથવા કહેવામાં આવેલ કોઇપણ એપ્લિકેશન ડાઉનલોડ કરશો નહીં.

ગુગલ કસ્ટમર કેર નંબર સર્ચ ફ્રોડ:

ગુગલ પર ઓનલાઇન કસ્ટમર કેર નંબર સર્ચ કરો ત્યારે છેતરપીંડી કરનારા દ્વારા વાસ્તવિક વેબસાઇટ જેવી જ ફેક વેબસાઇટ બનાવી તેમાં ગેરમાર્ગે દોરતી માહિતી, ફોન નંબર આપેલ હોય છે. વેબસાઇટની ચકાસણી કર્યા વગર આપેલ નંબર ઉપર જ્યારે ફોન કરવામાં આવે છે ત્યારે વાત થતી નથી અથવા અમારા એક્ઝ્યુકેટીવ તમોને ફોન કરશે તેવું જણાવવામાં આવે છે. ત્યારબાદ થોડા સમયમાં બીજા નંબર ઉપરથી ફોન આવે છે અને વાતચીતથી વિશ્વાસમાં લઇ તમારી અંગત/ બેંકની માહિતી મેળવી નાણાકીય છેતરપિંડી કરે છે.

- કંપનીના કસ્ટમર કેર નંબર તેની ઓફીશીયલ વેબ સાઇટ પરથી લઇને સંપર્ક કરવો.
- બેંક/ક્રેડિટ કાર્ડના તથા જરૂરી કસ્ટમર કેર નંબર પોતાના મોબાઇલમાં save કરી રાખો.
- એમેઝોન, સ્વીગી, ઝોમેટો જેવી એપ્લીકેશનમાં કસ્ટમર કેર નંબર તથા હેલ્પનું ઓપ્શન એપ્લિકેશનમાં જ આપેલ હોય છે તેનો ઉપયોગ કરો.

ઇન્સ્ટન્ટ લોન એપ્લિકેશન ફ્રોડ:

જરૂરીયાતમંદ લોકો જ્યારે ઓનલાઇન લોન અંગે સર્ચ કરે છે ત્યારે ઓનલાઇન ઘણી બોગસ ઇન્સ્ટન્ટ લોન એપ્લિકેશન જોવા મળે છે. આ એપ્લિકેશન ઓછા દસ્તાવેજ ઉપર નાની રકમની ઇન્સ્ટન્ટ લોન ઓફર કરે છે. એપ્લિકેશન ડાઉનલોડ કરતા સમયે તેઓ તમારા મોબાઇલની ગેલેરી, ફાઇલો, કોન્ટેક્ટ લીસ્ટ બધું એક્સેસ કરવાની પરમિશન માંગે છે. જે પરમિશન એલાઉ કરતા જ તેઓ પાસે તમારો ડેટા જતો રહે છે. ત્યારબાદ તેઓ તમોને વ્યાજ સાથે રકમ અઠવાડીયામાં ભરવા જણાવે છે અને સાથે તમારા ફોટા મોર્ફ કરી તમારા કોન્ટેક્ટ લીસ્ટના લોકોને મોકલી આપે છે અથવા ફોન કરે છે અને આપને હેરાન-પરેશાન કરે છે.

- RBI દ્વારા માન્યતા પ્રાપ્ત હોય તેવી જ લોન એપ્લિકેશન ડાઉનલોડ કરવી.
- કોઇપણ એપ્લિકેશન ડાઉનલોડ કરતા સમયે કોન્ટેક્ટ અને ફોટો ગેલેરીના એક્સેસની પરમિશન એલાઉ કરવું નહીં.
- કોઇપણ પ્રકારની અજાણી એપ્લિકેશન/ લિન્ક ઉપર ક્લિક કરવું નહીં.

ક્રિપ્ટો કરન્સી ફ્રોડ:

સાયબર ક્રિમિનલ્સ દ્વારા ઓનલાઇન સોશિયલ મીડિયા પર જાહેરાત આપવામાં આવે છે અથવા SMS/Whatsapp ઉપર મેસેજ મોકલવામાં આવે છે કે, ક્રિપ્ટો કરન્સીમાં રોકાણ કરવાથી ઓછા સમયમાં ખુબ સારૂ વળતર મેળવો. જે લોકો તેઓનો સંપર્ક કરે તેઓને ફેક ક્રિપ્ટો કરન્સી ટ્રેડિંગ વેબસાઇટ અથવા એપ્લિકેશન ડાઉનલોડ કરાવી તેમાં એકાઉન્ટ ખોલાવડાવી રોકાણ કરેલ રકમનું ઉંચુ વળતર બતાવવામાં આવે છે પરંતુ નાણા વિડ્રો કરવા દેવામાં આવતા નથી. ઘણા કિસ્સામાં નાણા મેળવી ક્રિપ્ટો કરન્સી આપવામાં આવતી નથી.

- આવા મેસેજનો કોઇ પ્રતિભાવ આપશો નહીં.
- આવી કોઇ અપ્લીકેશન ડાઉનલોડ કરવી નહી.
- આવી અપ્લીકેશનમાં ઉચું વળતર જોઇ લલચાવું નહી.

ઈલેક્ટ્રીસીટી બીલ ફ્રોડ:

ગુનેગારો દ્વારા જો તમારૂ બીલ અપડેટ કરવામાં નહીં આવે તો તમારી વીજળી અમુક કલાકો પછી બંધ થઇ જશે જેથી ઇલેક્ટ્રીસીટી ઓફિસરનો આપેલ નંબર ઉપર ફોન કરવા જણાવે છે. જે લોકો આપેલ નંબર ઉપર સંપર્ક કરે તેઓની સાથે બીલ ભરવાના બહાને નાણાકીય છેતરપીંડી કરવામાં આવે છે.

- આવા મેસેજનો કોઇ પ્રતિભાવ આપશો નહીં.
- ખાતરી કરવા માટે ઈલેક્ટ્રીક કંપનીની કાયમી ઓફિસની મુલાકાત પણ લઈ શકો છો.
- બીલની વિગતો કંપનીની સત્તાવાર વેબસાઇટ ઉપર ચકાશો, ઉતાવળમાં ક્યારેય રકમ ચૂકવવી નહીં.

મેટ્રીમોનીયલ ફ્રોડ:

છેતરપિંડી કરનાર વ્યક્તિ પોતાની ખોટી ઓળખ, ફોટો રાખી મેટ્રોમોનીયલ વેબસાઇટ્સ ઉપર રજીસ્ટ્રેશન કરાવે ત્યારબાદ સાઇટ ઉપર રજીસ્ટર અન્ય પુરુષ કે મહિલાઓનો સંપર્ક કરી મીઠી વાતો કરી મિત્રતા કેળવી સામેવાળી વ્યક્તિ ને વિશ્વાસમા લે છે અને કિંમતી ભેટ મોકલાવેલ છે તેવું ખોટું જણાવે છે. ત્યારબાદ કસ્ટમ વિભાગમાંથી બોલું છું તેવો ફોન આવે છે અને તમારી કિંમતી ભેટ છોડાવવા માટે કસ્ટમ ડ્યુટી, જી.એસ.ટી. તથા અલગ અલગ ડ્યુટી ભરવાના બહાને નાંણાકીય છેતરપિંડી કરવામાં આવે છે.

- પ્રમાણિત અને વિશ્વાસુ મેટ્રીમોનીયલ વેબસાઇટ ઉપર રજીસ્ટ્રેશન કરવું.
- તમારી અંગત માહિતી અથવા ફોટો share કરવા નહીં.
- અજાણ્યા ઇન્ટરનેટ મિત્ર ઉપર વિશ્વાસ રાખવો નહીં અને તેણે મોકલેલ ભેટ માટે કોઇ નાણા ચુકવવા નહીં.

લોન ફ્રોડ:

સાયબર ક્રિમિનલ્સ, લોન મેળવવા ઈચ્છુક લોકો દ્વારા કરવામાં આવતી ઓનલાઈન ઇન્કવાયરીના ડેટાને આધારે સીધો ફોન ઉપર સંપર્ક સાધીને લોન માટે લોભામણી સ્કીમ આપે છે અથવા સોશિયલ મીડિયા પ્લેટફોર્મ ઉપર જુદી જુદી બેંકમાથી ઓછા વ્યાજે લોન અપાવવાની લોભામણી જાહેરાત મૂકી ઇચ્છુક લોકો પાસેથી લોન અપાવવા રજીસ્ટ્રેશન, ટેક્સ, જીએસટી વગેરે ચાર્જ પેટે નાણા પડાવી લેતા હોય છે.

- હંમેશા કંપની/બેંકની ઓફિશીયલ વેબસાઇટ અથવા બ્રાન્ચ ઉપર જઇ આવી સ્કીમની ખરાઇ કરો.
- ઓનલાઇન મોકલવામાં આવેલ લોન એપ્રુવલ લેટરની ખરાઇ કરવી.

ઈન્સ્યોરન્સ ફ્રોડ:

છેતરપિંડી કરનાર વ્યક્તિ મોબાઈલ ફોન અથવા ઈમેઈલ દ્વારા સંપર્ક કરીને વ્યક્તિને વિશ્વાસમા લઇ એવુ જણાવે છે કે, તમારી કે તમારા કુટુંબીજનની જૂની વીમા પૉલીસી પાકી ગઇ છે અથવા વિમા પૉલીસીમાં સારુ રિફંડ મળે એમ છે એવી લૉભામણી/ ખોટી માહિતી આપી વિમાની પાકેલ રકમ મેળવવા માટે,વિમા રકમના ડિફરન્સ પેટે, સિક્યોરીટી ડિપોઝીટ પેટે,વિમાના પેનલ્ટી પેટે,વિમાની અલગ-અલગ કંપનીની ખોટી પોલીસી લેવડાવવાના બહાના હેઠળ નાણાની છેતરપીંડી કરે છે.

- વિમા પોલીસીના બોનસ અથવા પાકેલ રકમ બાબતના ફોનનો કોઇ પ્રતિભાવ આપશો નહીં.
- નજીકની વિમા કંપનીની ઓફિસમાં જઇ ચકાસણી કરવી.
- તમારા કુટુંબીજનો સાથે પોલિસી લીધેલ હતી કે કેમ તે અંગે ખાતરી કરો.

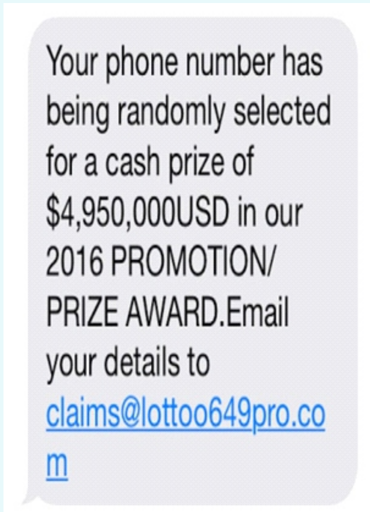
જોબફ્રોડ:

આરોપીઓ દ્વારા ઓનલાઇન ફેક વેબસાઇટ બનાવી અથવા SMS દ્વારા કે અખબારમાં નોકરી માટે લોભામણી જાહેરાત આપી નોકરી મેળવવા ઇચ્છુક લોકો દ્વારા ઓનલાઈન સબમીટ કરવામાં આવેલ માહિતી મેળવીને ફોન અથવા ઈમેઈલ દ્વારા સંપર્ક સાધીને તેમને લોભામણી ખોટી માહિતી આપી, ટેલિફોનીક ઇન્ટરવ્યુ લઇને કે ઇ-મેઇલ દ્વારા નોકરી મળી ગઇ છે તે પ્રકારે વિશ્વાસમા લઇ અલગ અલગ પ્રોસેસીંગ ફી ના બહાના હેઠળ અથવા તેઓ ઝડપથી ફી નહિ ભરો તો નોકરી જતી રહેશે એવો ભય વતાવી પૈસા પડાવી છેતરપિંડી કરે છે.

- કોઇપણ કંપની નોકરી આપવા નાણાની માંગણી કરતી નથી. હંમેશા કંપનીની વેબસાઇટના સ્પેલિંગ ચેક કરવા તથા
- મોકલવામાં આવેલ જોબ લેટરમાં સ્પેલિંગ ચેક કરવા તથા લેટરમાં આપેલ સાઇનની ખરાઇ કરવી.
- નોકરીની લાલચમાં આવી ઉતાવળે નાણા ચુકવણી કરવી નહિ.

લૉટરી ફ્રોડ:

તમારો મોબાઇલ નંબર સિલેક્ટ થયો છે અને તમને KBC માં અથવા અન્ય નામ આપી ખુબ મોટી રકમની લૉટરી લાગી છે તેવા મેસેજ/ ઇ-મેઇલ મોકલી લૉટરીની રકમ મેળવવા ફોન ઉપર સંપર્ક કરવા અથવા લીંક ઉપર ક્લિક કરવા જણાવે છે. જે સંપર્ક કરે તેઓ પાસેથી તેઓના આધારકાર્ડ, બેંક એકાઉન્ટ તથા ફોટો માંગે છે અને ત્યારબાદ લૉટરી રકમ મેળવવા માટે જુદા જુદા ચાર્જ ભરવાનું જણાવી છેતરપીંડી કરવામાં આવે છે.



- જો તમોને આવા કોઇ મેસેજ આવે તો તેનો કોઇ પ્રતિભાવ આપવો નહીં.
- તમારી અંગત માહિતી જેવી કે, આધારકાર્ડ, બેંક એકાઉન્ટ નંબર કે ફોટા કે નાણા આપવા નહીં.

OLX ફ્રોડ:

નાગરીકો દ્વારા પોતાની વસ્તુ OLX પર વેચાણ કરવા જાહેરાત મુકવામાં આવે ત્યારે ઘણીવાર અજાણી વ્યક્તિ પોતે આર્મીમાં છું તેવી બનાવટી વાતો કરી વસ્તું ખરીદવા માટે એડવાન્સ ચૂકવણી વૉલેટ દ્વારા કરવાનો આગ્રહ રાખે છે અને એક QR કોડ મોકલી સ્કેન કરવાનું કહે છે, ભોગ બનનાર જ્યારે QR કોડ સ્કેન કરે છે ત્યારે નાણા મળવાની જગ્યાએ એના ખાતામાંથી નાણા જતા રહે છે.

- નાણા મેળવવા ક્યારેય QR કોડ સ્કેન કરવાનો હોતો નથી અથવા કોઇ UPI PIN/પાસવર્ડ આપવાનો હોતો નથી.
- હંમેશા વેચનાર/ખરીદનારને રૂબરૂ મળવાનો આગ્રહ રાખો.
- યાદ રાખો સોશ્યલ મીડિયા પ્લેટફોર્મ પર આર્મીમેન તરીકે ઓળખ આપનાર આર્મીમાં હોય તે જરૂરી નથી.

પોન્ઝી સ્કીમ ફ્રોડ:

છેતરપીંડી કરનાર લોકો દ્વારા આકર્ષક જણાઇ આવતી અવાસ્તવિક એવી લોભામણી જાહેરાતો જેવી કે ઓછા સમયમાં નાણા ડબલ થશે, ઉંચા વ્યાજદર મળશે તેવું જણાવવામાં આવે છે. જ્યારે કોઇ તેઓનો સંપર્ક કરે છે અથવા આપેલ લીંક ઉપર ક્લિક કરે છે ત્યારે કોઇ ફેક એપ્લિકેશન ડાઉનલોડ કરાવી શરૂઆતમાં રોકેલ નાની રકમનું સારૂ વળતર આપી મોટી રકમ રોકવા જણાવે છે. જે રકમનું તેઓના એકાઉન્ટમાં સારા એવા નફા સાથે ખોટી રીતે બેલેન્સ બતાવવામાં આવે છે અને નાણા વિડ્રો કરવા અલગ-અલગ ચાર્જ ભરાવી નાણા વિડ્રો કરવા દેવામાં આવતા નથી અને છેતરપિંડી કરવામાં આવે છે.

- સોશિયલ મીડિયા ઉપર આવી લોભામણી જાહેરાત જોઇ લલચાવું નહીં સંપર્ક કરવો નહીં.
- તેઓ દ્વારા મોકલવામાં આવતા ઉંચા વળતરના ફોટા ઉપર વિશ્વાસ કરવો નહીં હંમેશા કંપની વિષે રીસર્ચ કરવું.

સીમ સ્વેપિંગ ફ્રોડ:

ગુનેગાર દ્વારા ફીશીંગ, વિશીંગ અથવા SMS દ્વારા લીંક મોકલી આપની અંગત માહિતી મેળવી લેવામાં આવે છે. ત્યારબાદ તેઓ સર્વિસ પ્રોવાઇડર પાસે તમારા સીમને બ્લોક કરાવી. સર્વિસ પ્રોવાઇડરને ત્યાં રૂબરૂ જઇ નવું સીમકાર્ડ મેળવી લે છે. ત્યારબાદ તમારા મોબાઇલ સાથે જોડાયેલ બેંક એકાઉન્ટ માંથી નાણાની ઉચાપત કરવામાં આવે છે.

- ઓનલાઇન અજાણ્યા લોકોને કોઇપણ કારણોસર તમારી અંગત માહિતી, દસ્તાવેજ આપશો નહીં.
- ફોનનુ નેટવર્ક અમુક કલાકો સુધી જતુ રહે તો તુરંત તમારા મોબાઇલ સર્વિસ પ્રોવાઇડરનો સંપર્ક કરી ચકાસણી કરો કે નવું સીમ કોઇને આપવામાં તો આવેલ નથી.

ઇન્કમટેક્ષ રીફંડ ફ્રોડ:

ગુનેગારો દ્વારા આપનું ઇન્કમટેક્ષ રીફંડ પ્રોસેસમાં છે જેથી રીફંડ મેળવવા આપેલ લીંક પર ક્લિક કરો તેવા ફેક મેસેજ મોકલવામાં આવે છે. લીંક ઉપર ક્લિક કરવાથી તેઓ તમારા બેંક એકાઉન્ટની તેમજ અંગત માહિતી મેળવી નાણાકીય છેતરપીંડી કરે છે.

- આવા મેસેજનો કોઇ પ્રતિભાવ આપશો નહીં. આપેલ લીંક ઉપર ક્લિક કરવું નહીં.
- જો લીંક ઉપર ક્લિક થઇ જાય તો તમારી અંગત તથા બેંકની વિગતો આપશો નહીં.
- તમે ચકાસો કે તમે રીફંડ માટે કોઇ રીટર્ન ભરેલ છે કે કોઇ કાર્યવાહી કરેલ છે.

ઓનલાઇન ગેમિંગ ફ્રોડ:

ઓનલાઇન ગેમિંગનો વ્યાપ વધવાથી સાયબર ક્રિમિનલ્સ દ્વારા પોપ્યુલર ગેમની વેબસાઇટ હોય તેવીજ ફેક વેબસાઇટ બનાવી તમારા બેંક એકાઉન્ટ, ક્રેડિટ કાર્ડ નંબર તથા અન્ય ઓનલાઇન એકાઉન્ટની લોગ-ઇનની માહિતી મેળવી ઓનલાઇન ગ્રે માર્કેટમાં વેચવામાં આવે છે. ઘણા કિસ્સામાં ચેટિંગ દ્વારા મિત્રતા કેળવી માહિતી મેળવી લેવામાં આવે છે. જે ગેમિંગ એકાઉન્ટના વધુ paying પ્રેક્ષકો હોય તેઓના એકાઉન્ટને ટારગેટ કરી હેક કરવામાં આવે છે. ઓનલાઇન ગેમમાં ફેક ઓફરો આપી નાણાની છેતરપીંડી કરવામાં આવે છે.

- ક્યારેય ગેમ ડાઉનલોડ કરવા ઇ-મેઇલ થી કે SMS દ્વારા કોઇ લીંક મોકલવામાં આવે તો ક્લિક કરશો નહીં.
- ગેમ રમતા કોઇ અજાણ્યા સાથે ચેટીંગ કરશો નહીં કોઇ હેરાન કરે તો તેને બ્લોક કરો અને રિપોર્ટ કરો.
- ઓનલાઇન ગેમ માટે કોઇ સસ્તી ઓફર આપે તો ગેમની બહાર કોઇ નાણાકીય વ્યવહાર કરવો નહીં.
- તમારા ગેમિંગ એકાઉન્ટમાં ટુ ફેક્ટર ઓથેન્ટિકેશન એક્ટિવેટ રાખો.

ફ્રેન્ડશીપ ક્લબ ફ્રોડ:

યુવતીઓ સાથે મિત્રતા કરવા અને તેમની સાથે સમય પસાર કરી નાણા કમાવા ફ્રેન્ડશીપ ક્લબમાં જોડાવો તેવી જાહેરાત સમાચાર પત્રમા આપવામા આવે છે અથવા SMS મોકલવામાં આવે છે. ઇચ્છુક લોકો સંપર્ક કરે ત્યારે રજીસ્ટ્રેશન માટે, યુવતી સાથે મુલાકાત માટે,સ્થળના બુકીંગ માટે એમ અલગ-અલગ કારણો આપી નાણા પડાવી છેતરપિંડી કરવામાં આવે છે.

- સમાચાર પત્રમાં આવી જાહેરાતો વાંચી સંપર્ક કરવો નહીં તથા આવા કોઇ SMS નો પ્રતિભાવ આપવો નહીં.
- ડેટીંગ વેબસાઇટ તથા ફ્રેન્ડશીપ ક્લબમાં રજીસ્ટ્રેશન માટે કોઇ નાણા ચુકવવા નહીં.

OTP આપ્યા વગર થતા ફ્રોડ: (કાર્ડ ક્લોનિંગ):

એટીએમ મશીનો/રેસ્ટોરન્ટ/પેટ્રોલ પંપ ઉપર તેમજ ઘણા સ્થળોએ POS મશીનમાં સ્કીમર લગાડ્યા હોય છે. જે તમારા ડેબીટ કાર્ડ/ક્રેડિટ કાર્ડનું ક્લોનીગ કરી તમારો ડેટા મેળવી લે છે અને તમારા દ્વારા નાંખવામાં આવેલ PIN નંબર જોઇ લીધા બાદ સ્કીમર મશીનથી ડેબીટ કાર્ડ/ક્રેડિટ કાર્ડ બનાવી નાણાકીય છેતરપીંડી કરવામાં આવે છે.

- એટીએમ મશીનમાં કોઇ સ્કીમર લગાડેલ છે તે ચકાસવું તેમજ એટીએમ સેન્ટરમાં બીજા કોઇને ઉભા રહેવા દેવા નહીં.
- રેસ્ટોરન્ટ/પેટ્રોલ પંપ ઉપર POS મશીન પોતાની પાસે મંગાવી ચેક કરી કાર્ડ આપવું.

સોશિયલ મીડિયા સંબંધિત ફ્રોડ

સાયબર બુલિંગ/બ્કેલમેલીંગ:

કોઇ વ્યક્તિ દ્વારા બીજી કોઇપણ વ્યક્તિને ઇલેક્ટ્રોનિક સંદેશા-વ્યવહારનો ઉપયોગ કરી ધમકાવવા, ડરાવવા, અપમાન કરવા કે ઉતારી પાડવા, મજાક ઉડાવવાના હેતુથી મેસેજ, વિડિયો, ફોટા મોકલવામાં આવે તેને સાયબર બુલિંગ કહે છે.

- અજાણ્યા લોકોની ફ્રેન્ડ રીક્વેસ્ટ સ્વીકારશો નહી.
- ઓનલાઇન સોશિયલ મિડીયા પ્લેટફોર્મ પર તમારી અંગત માહિતી શેર કરશો નહીં.
- ઓનલાઇન કંઇપણ પોસ્ટ કરતા પહેલા થોભો અને વિચારો.
- જો તમે સાયબર બુલિંગનો ભોગ બનો તો તુરંત માતા-પિતાને જાણ કરો તથા નજીકના પોલીસ સ્ટેશનનો સંપર્ક કરો.
- તમારી ખૂબજ અંગત મિત્રો/સહેલીઓ સાથે પણ સોશિયલ મિડીયા પ્લેટફોર્મના પાસવર્ડ શેર કરોન કરો.

સાયબર સ્ટોકિંગ

કોઇ વ્યક્તિ દ્વારા કોઇપણ વ્યક્તિનો ઇલેક્ટ્રોનિક માધ્યમનો ઉપયોગ કરી પીછો કરી, સોશિયલ મીડિયા પરની દૈનિક પ્રવૃત્તિઓ જાણી, તેની વ્યક્તિગત માહિતી એકત્રિત કરી ઇમેઇલ, સોશિયલ મીડિયા, ચેટ રૂમ, ઇન્સ્ટન્ટ મેસેજિંગ દ્વારા પરેશાન અથવા ધમકી આપવા જેવી કાર્યવાહી કરવામાં આવે તેને સાયબર સ્ટોકિંગ કહે છે.

સોશિયલ મીડિયા પર પોતાની તમામ પ્રવૃતિને અપલોડ કરવાથી કોઇ અજાણ્યા વ્યક્તિ આપની તમામ પ્રવૃતિ પર નજર રાખી તેનો દુરૂપયોગ કરી શકે છે.

- સોશિયલ મીડિયા પ્રોફાઇલ પ્રાઇવેટ અને લોક રાખો.
- તમારી દરેક એક્ટિવીટીને સોશિયલ મીડિયા પર અપલોડ કરશો નહીં.
- જાહેર સ્થળોના wifi નો ઉપયોગ કરવાનું ટાળો.

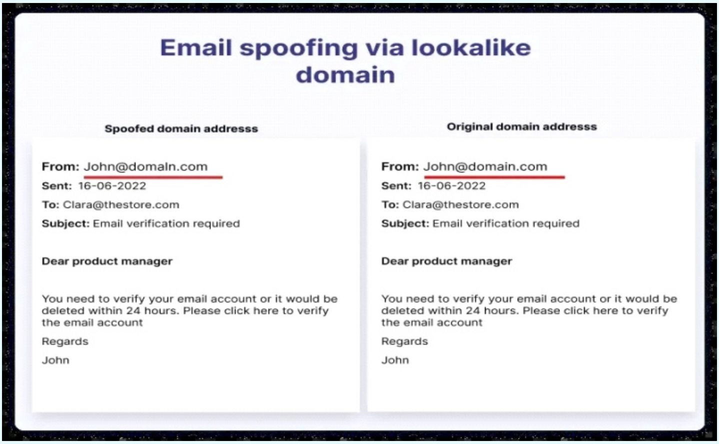
આઇડેન્ટીટી થેફ્ટ:

તમારી અંગત માહિતી જેવીકે, સરનામું, ફોન નંબર, ઇ-મેઇલ એડ્રેસ, લોગ ઇન આઇડી, પાસવર્ડ, ક્રેડિટ કાર્ડની માહિતી, બેંક એકાઉન્ટ નંબર વિગેરે સાયબર ક્રિમિનલ્સ દ્વારા સોશિયલ એન્જીનિયરીંગથી, ઇ-મેઇલ, SMS દ્વારા લીંક મોકલી મેળવી તેનો ગેરકાયદેસર રીતે નાણાકીય ફાયદો મેળવવા ઉપયોગ કરવામાં આવે તેને આઇડેન્ટીટી થેફ્ટ કહે છે.

- તમારા પાસવર્ડ ઓછામાં ઓછા આઠ અક્ષરોનો જેમાં એક કેપિટલ લેટર, સ્મોલ લેટર, ન્યુમેરિક નંબર અને સિમ્બોલ હોય તેવા રાખો અને નિયમિત બદલતા રહો.
- અજાણ્યા વ્યક્તિ દ્વારા ઇ-મેઇલ, SMS મારફતે મોકલવામાં આવેલ લીંક ઉપર ક્લિક કરશો નહીં.
- તમારા ઉપકરણમાં સિક્યુરીટી સોફ્ટવેર રાખો અને તમામ એપ્લિકેશન અપડેટ રાખો.

ઈ-મેઈલ સ્પુફિંગ ફ્રોડ:

ઇ-મેઇલનો ઉપયોગ મહત્વપૂર્ણ માહિતી/વર્ક ઓર્ડર/પેમેન્ટ ડીટેઈલ વગેરે ઝડપથી શેર કરવા માટે થાય છે ત્યારે સાયબર ગઠીયાઓ ઇમેઇલ આઇડીની ચોક્કસ પ્રતિકૃતિ બનાવે છે અથવા ઇમેઇલ સ્પુફ કરવા માટે સમાન શબ્દોનો ઉપયોગ કરે છે. છેતરપિંડી કરનારાઓ માલ માટેની ડિલિવરી પદ્ધતિમાં ફેરફાર કરીને લાભ મેળવવાનો પ્રયાસ કરે છે અથવા તેઓ જ્યાં પૈસા જમા કરાવવાના છે તે બેંક ખાતાની વિગતો પણ બદલી શકે છે. છેતરપિંડીના ભાગરૂપે, આરોપી જુદા જુદા બહાના હેઠળ ભંડોળ ફેરવવાનો અથવા પૈસા માંગવાનો પણ પ્રયાસ કરે છે.



- ઇ-મેઇલ દ્વારા મોકલવામાં આવેલ અજાણી શંકાસ્પદ લીંક પર ક્લીક કરશો નહીં.
- હંમેશા ઈ-મેઈલ એડ્રેસ અને વેબસાઈટ યુઆરએલમાં સ્પેલીંગ ધ્યાનથી ચેક કરો.
- સ્પામ ફિલ્ટર્સ એક્ટીવ કરીને તમારી ઇમેઇલ સુરક્ષામાં વધારો કરો.

રેન્સમવેર:

રેન્સમવેર એક malicious સોફ્ટવેર (માલવેર) છે. અજાણ્યા વ્યક્તિ દ્વારા આવેલ ઇ-મેઇલ પર ક્લિક કરવાથી અથવા મોકલવામાં આવેલ લીંક ઉપર ક્લિક કરવાથી આ માલવેર તમારા કોમ્પ્યુટરમાં રહેલ ફાઇલો તથા ડેટાને એન્ક્રિપ્ટ કરે છે જેથી આપ ફાઇલોનો ઉપયોગ કરી શકતા નથી. ત્યારબાદ ઇ-મેઇલ મોકલનાર દ્વારા ફાઇલો ડિક્રિપ્ટ કરવા માટે ખંડણી માંગવામાં આવે છે અને સામાન્ય રીતે બીટકોઇન/ડોલરમાં ચુકવવા જણાવવામાં આવે છે.

- જ્યારે કોમ્પ્યુટરનો ઉપયોગ કરતા ના હોવ ત્યારે ઇન્ટરનેટનું જોડાણ કાઢીને રાખો.
- નિયમિત ડેટાનો બેક-અપ લેતા રહો.
- અજાણ્યા સ્રોત તરફથી આવેલ ઇ-મેઇલ ઉપર અથવા લીંક પર ક્લિક કરશો નહીં.
- ફાઇલ ડિક્રિપ્ટ કરવા કોઇ ખંડણી ચુકવશો નહીં.

WhatsApp પ્રાઈવસી સેટિંગ

Make sure you are logged out from not in use device.
Go to Three Dots >WhatsApp Web> Log Out from all Devices
Always use Two-step verification
Go to Settings >Account>Two-Step Verification
Do hide your last seen
Go to Settings> Account>Privacy>Last Seen>Nobody
Hide your profile picture and about
Go to Settings>Account >Privacy>Profile Picture/About > Nobody /My Contacts
Do turn off Read Receipts
Go to Settings>Account>Privacy>Read Receipts
Do change the setting of group chat so that no one unknown can add you.
Go to Settings>Account>Privacy>Groups>My Contacts

Facebook પ્રાઈવસી સેટિંગ

Make sure to Logout on Unwanted Device
Go to Setting & privacy>Setting>Security & Login
Always use two factor Authentication
Go to Setting & privacy>Setting>Security & Login> Two factor Authentication
Make sure you have set up Login Alerts
Go to Setting & privacy>Setting>Security & Login> Get Alerts about unrecognized Login
Make sure you are using safe browsing
Go to Setting & privacy>Setting>Security & Login> safe browsing
Do lock your profile
Go to Setting & privacy>Setting>profile locking
Do turn on the face recognition feature
Go to Setting & privacy>Setting>face recognition

Instagram પ્રાઈવસી સેટિંગ

Do setup Two-Step Verification
Go to Setting>Security>Two-Factor Authentication
Make sure you have a Private Account
Go to setting>Privacy>Privacy Account (make it on)
Choose wisely who can Tag you
Go to Settings>privacy>tags(Turn on Manually approve Tags)
Don't get yourself in suggestions to other people
Go to Settings>Account>Contacts syncing
Do remove access on unnecessary Apps& Websites
Go to Setting>Security>Apps& websites
Don't let people know your Active status
Go to setting>Privacy>Activity status(turn it off)

SnapChat પ્રાઈવસી સેટિંગ

Enable Two-factor authentication
→Go to your Profile > Settings, then tap the button beside SMS Verification to turn it on
Make Sure who Can Contact You
→To do this, go to **Settings**, look for the **Contact Me option** under the Who can... Heading, and tap My Friends so a checkmark appears next to it.
Select Who You Want to See Your Stories
→Go to **Settings** Scroll down to the **View My Story**. Then, you can select Everyone, My Friends or build a custom list.
Hide Yourself from the Quick Add Section
→Profile > Settings (gear icon) and selecting See Me in Quick Add.

સોશિયલ મીડિયા ક્રાઈમથી બચવા માટેની ટીપ્સ:

- અજાણ્યા લોકો સાથે તમારી વ્યક્તિગત માહિતી /અંગત ફોટા શેર કરશો નહીં.
- અજાણ્યા લોકો તરફથી આવતી ફ્રેન્ડ રિક્વેસ્ટ/વિડિયો કોલ સ્વીકારશો નહીં.
- તમારા સોશિયલ મીડિયા એકાઉન્ટમાં ટુ સ્ટેપ વેરીફિકેશન એક્ટિવેટ રાખો.
- તમારી દરેક એક્ટિવીટીને સોશિયલ મીડિયા ઉપર જાહેર કરશો નહીં.
- સોશિયલ મીડિયા એકાઉન્ટસની પ્રોફાઇલ લોક તથા પ્રાઇવેટ રાખો.
- પાસવર્ડ ઓછામાં ઓછા આઠ અક્ષરોનો રાખો જેમાં કેપિટલ લેટર, સ્મોલ લેટર, સંખ્યા અને સિમ્બોલ હોય તેવો રાખો અને પાસવર્ડ કોઇને પણ આપશો નહીં તથા નિયમિત સમયાંતરે બદલતા રહો.
- લોભામણી જાહેરાતો જોઇ લલચાવું નહીં જે- તે કંપની/રેસ્ટોરન્ટની ઓફિશીયલ વેબસાઇટ ઉપર જઇ ખરાઇ કરવી.
- પોર્નોગ્રાફી વેબસાઇટ જોવી નહીં તેમજ ચાઇલ્ડ પોર્નોગ્રાફીને લગતો કોઇ વિડિયો/ઇમેજ ડાઉનલોડ કરવી નહીં કે ફોરવોર્ડ કરવી નહીં.
- સોશિયલ મિડીયા પ્લેટફોર્મ ઉપર કોઇપણ મેસેજ ખરાઇ કર્યા સિવાય ફોરવોર્ડ કરશો નહીં. [ફેક મેસેજ ચેક કરવા માટે **PIBFactCheck**નો ઉપયોગ કરો]
- જો તમને ઓનલાઇન કંઈક અયોગ્ય દેખાય તો તુરંત પુખ્ત વ્યક્તિને જાણ કરો.

નાણાકીય છેતરપિંડીથી બચવા માટેની ટીપ્સ:

- **R B I** દ્વારા માન્યતા પ્રાપ્ત હોય તેવી જ ઇન્સ્ટન્ટ લોન એપ્લિકેશન ડાઉનલોડ કરવી અને જરૂરી હોય એટલીજ પરમીશન **Allow** કરવી.
- ક્યારેય કોઈ સાથે **OTP/PIN/CVV** નંબર **share** કરશો નહિ. બેંક ક્યારેય ગ્રાહકોને આવી વિગતો ફોન/મેસેજથી પૂછતી નથી.
- અજાણ્યા વ્યક્તિ દ્વારા મોકલવામાં આવેલ લિંક પર ક્યારેય ક્લિક કરશો નહિ.
- ક્રિપ્ટો કરન્સી અથવા ફોરેક્સ ટ્રેડીંગમાં રોકાણ કરવાથી ઓછા સમયમાં ખુબ ઉંચુ વળતર મળશે એવી જાહેરાત/ મેસેજ માટે કોઇ પ્રતિક્રિયા આપશો નહીં.
- અજાણ્યા વ્યક્તિના કહેવાથી **Any Desk, Team Viewer, Quick Support** જેવી એપ્લિકેશન ડાઉનલોડ કરશો નહિ.
- હંમેશા કંપની/ બેંકની ઓફિસીયલ વેબસાઇટ અથવા એપ્લિકેશનમાંથી જ કસ્ટમર કેર નંબર શોધો.
- તમારો મોબાઇલ નંબર હંમેશા તમારી બેંક એકાઉન્ટ સાથે લિંક રાખો અને બેંકનો કસ્ટમર કેર નંબર **contact** લીસ્ટમાં **save** રાખો.
- પૈસા મેળવવા **UPI** પીન આપશો નહીં, **QR** કોડ સ્કેન કરશો નહિ.
- ઇલેક્ટ્રીસિટી બીલ ભરવાના/ લોટરી જીત્યાના/આવકવેરા રિફંડ માટે આવતા **SMS**/વોટ્સ એપ મેસેજના જવાબ આપશો નહીં.
- જાહેર વાઇ-ફાઇ નો ઉપયોગ કરી ક્યારેય કોઇપણ બેંકિંગ વ્યવહાર કરશો નહિ.
- ટેલિગ્રામ, વોટ્સએપમાં પ્રાઈવસી સેટિંગ એ રીતે રાખો કે અજાણી વ્યક્તિઓ તમને કોઈ ગૃપમાં એડ કરી શકે નહિ.

સાયબર ક્રાઇમ સેલની સિદ્ધીઓ

❖ **ફેક વેબસાઇટ બનાવી છેતરપીંડી આચરનાર <u>આફ્રિકન ગેંગનો પર્દાફાશ:</u>**

ભારતની અલગ અલગ પ્રખ્યાત હોસ્પીટલોના નામની ફેક વેબસાઇટ તથા આર. બી. આઇ. નામના ફેક ઇ- મેઇલ આઇ. ડી. બનાવી છેતરપીંડી આચરનાર **કુલ- ૦૩ આફ્રિકન આરોપી સહિત કુલ-૦૪ આરોપીઓને** શોધી કાઢી ફરિયાદી દ્વારા **કુલ-૦૬** એકાઉન્ટમાં જમા કરાવેલ **રૂ.૧૪,૭૮,૪૦૦/- પૈકી કુલ રૂ.૯,૬૦,૪૬૧/- ફ્રીઝ** કરવામાં આવેલ છે

❖ **સિમ સ્વેપ તથા ઇ-મેઇલ હેકીંગ કરી નાણા ટ્રાન્સફર કરનાર <u>નાઇજીરીયન ગેંગનો પર્દાફાશ:</u>**

બેંક તથા કેશ ક્રેડિટ એકાઉન્ટમાં રજીસ્ટર મોબાઇલ બંધ કરી સિમ સ્વેપ તથા ઇ- મેઇલ હેક કરી બંને એકાઉન્ટમાંથી **રૂ.૧,૭૧,૮૦,૦૧૨/- NEFT/RTGS** થી અલગ અલગ બેંક એકાઉન્ટોમાં ટ્રાન્સફર કરી છેતરપીંડી કરેલ હતી. જે ગુન્હામાં સંડોવાયેલ **કુલ- ૨ નાઇજીરીયન** આરોપીઓ સહિત **કુલ-૦૬** આરોપીઓને શોધી કાઢી તેઓ પાસેથી રોકડા **રૂ.૫,૯૦,૫૦૦/-** રીકવર કરવામાં આવેલ છે.

❖ **પોલીસી ફ્રોડ કરતી <u>દિલ્હીની ગેંગનો પર્દાફાશ:</u>**

વીમાની પાકતી રકમ મેળવવા ગવર્મેન્ટ ઓફ ઇન્ડીયા સાથે જોડાયેલા છે તેવી ખોટી ઓળખાણ આપી વીમા કંપનીઓમાં **કુલ રૂ.૪૮,૩૫,૯૧૦/-** ની ખોટી પોલીસી લેવડાવી છેતરપીંડી આચરતી ઉત્તરપ્રદેશ તથા દિલ્હી ખાતેથી **કુલ-૦૪ આરોપીઓને** અટક કરેલ અને આરોપીઓ પાસેથી **રોકડા કુલ રૂ.૧૨,૨૫,૦૦૦/- રીકવર** કરવામાં આવેલ છે.

❖ **RBL ક્રેડિટ કાર્ડના નામે છેતરપીંડી કરતી જામતારા ગેંગનો પર્દાફાશ:**

આરોપીઓ દ્વારા **RBL** બેંક ક્રેડિટ કાર્ડના ધારકો સાથે **OTP** મેળવી છેતરપીંડી કરનાર ઝારખંડના જામતારા ખાતેથી **કુલ-૧** તથા સ્થાનિક **કુલ- ૬** ઇસમોને અટક કરી આરોપીઓના બેંકોના **કુલ- ૧૧૫** એકાઉન્ટ માંથી કુલ **રૂ. ૬૭, ૯૭, ૫૪૬/ - ફ્રીઝ** કરવામાં આવેલ છે.

સુરત શહેરમાં નોંધાયેલ **કુલ-૭** તથા અમદાવાદ શહેરના **કુલ- ૧** ગુના શોધી કાઢવામાં આવેલ છે.

❖ **ઇન્વેસ્ટમેન્ટના નામે ફ્રોડ કરતી પશ્ચિમ બંગાળની ગેંગનો પર્દાફાશ:**

ફરીયાદીશ્રીને વિશ્વાસમાં લઇ આ એપ્લીકેશનમાં ઇન્વેસ્ટ કરવાથી પ્રોફીટ થશે તેવી લોભામણી લલચામણી વાતો કરી **રૂ. ૩, ૫૬, ૭૭૫/ - ની** છેતરપીંડી કરનાર પશ્ચિમ બંગાળ, જલપાઇગુરી થી **એક મહીલા** આરોપીને અટક કરેલ છે.

❖ **ફેક વેસબાઇટ બનાવી છેતરપીંડી આચરતી વેસ્ટ આફ્રિકન ગેંગનો પર્દાફાશ:**

ઓનલાઇન વેબસાઇટ ઉપર ગલુડીયું વેચવાની જાહેરાત મુકી ગલુડીયું ખરીદ કરવા સંપર્ક કરતા અલગ અલગ ચાર્જ પેટે રૂ.૮,૬૨,૨૦૦/- છેતરપીંડી આચરનાર કુલ-૦૨ વેસ્ટ આફ્રિકન આરોપીને અટક કરી આરોપીઓના બેંક એકાઉન્ટમાં કુલ રૂ.૪,૦૦,૦૦૦/- ફ્રીઝ કરવામાં આવેલ છે.

❖ **વીડિયો કોલ કરીને Sextortion આચરતી <u>મેવાતી ગેંગનો પર્દાફાશ:</u>**

આરોપી દ્વારા ઇન્સ્ટાગ્રામ ઉપર મહિલાના નામે ફેક એકાઉન્ટ બનાવી ભોગ બનનારને વીડિયો કોલ કરી બિભત્સ વીડીયો બનાવી વીડિયો વાયરલ કરવાની ધમકી આપી બળજબરીથી **રૂ. ૨૦,૦૦૦/-** પડાવી વધુ રૂપિયાની માંગણી કરતા ભોગ બનનારે આપઘાત કરેલ હતો. આ ગુન્હામાં સંડોવાયેલ **આરોપીને**

❖ **આર.ટી.ઓ. કચેરી, સુરત શહેર ખાતેથી ડ્રાઇવીંગ ટેસ્ટ લીધા વગર પાકુ લાયસન્સ એપ્રુવ કરનાર ગેંગનો પર્દાફાશ:**

સુરત આર.ટી.ઓ. કચેરીની કોમ્પ્યુટર સીસ્ટમમાં આર.ટી.ઓ. કચેરીની પરવાનગી વગર ગેરકાયદેસર રીતે પ્રવેશ કરી સીસ્ટમ સાથે ચેડા કરી બારોબાર **ડ્રાઇવીંગ ટેસ્ટ લીધા વગર પાકુ લાયસન્સ એપ્રુવ કરતી ગેંગના કુલ-૦૫ આરોપીઓને** સુરત ખાતેથી અટક કરેલ છે.

❖ **ખોટી કંપનીઓ બનાવી જી.એસ.ટી. નંબરો મેળવી ગુન્હો આચરનાર આરોપીની અટકાયત:**

બેંક એકાઉન્ટ બંધ કરાવવાના બહાને ડોક્યુમેન્ટ મેળવી તથા બોગસ **NO OBJECTION CERTIFICATE** તથા ફેક ઇ-મેઇલ આઇડી બનાવી **ખોટી કંપનીઓ બનાવી પાનકાર્ડ ઉપર બે જી.એસ.ટી. નંબરો મેળવી રૂપીયા વીસ કરોડના ટ્રાન્જેક્શન** બતાવી છેતરપીંડી કરનાર **કુલ-૦૧ આરોપીને** અટક કરેલ છે.

- **GSRTC બસની ટ્રીપો ઓનલાઇન કેન્સલ/એડહોક કરી GSRTC પાસેથી રીફંડ મેળવતા એજન્ટોના કૌભાંડનો પર્દાફાશ:**

  GSRTCના યુઝરનેમ તથા પાસવર્ડનો ગેરકાયદેસર રીતે ઉપયોગ કરી તેઓના કુલ-૬૦ ટ્રીપ એડહોક/કેન્સલ કરી **GSRTC** દ્વારા માન્યતા પ્રાપ્ત કુલ-૧૧ એજન્ટોએ રીફંડ મેળવી લઇ **GSRTC** ને **કુલ રૂ.૬,૧૨,૮૧૩/-** નું નુકસાન કરાવી ગુન્હો આચરેલ. આ ગુન્હામાં દાહોદ અને જામનગર ખાતેથી **કુલ-૦૫ આરોપીઓને** અટક કરેલ.

- **સસ્તા ભાવે ક્રીપ્ટો કરન્સી USDT આપવાની લોભામણી લલચામણી વાતો કરી ક્રીપ્ટો કરન્સી USDT ન આપી છેતરપીંડી કરતી ગેંગનો પર્દાફાશ:**

  ફરિયાદી પાસેથી રૂ. ૨૯, ૫૦, ૦૦૦/ - મેળવી લઇ રૂ.૯,૫૦,૦૦૦/-ના ક્રીપ્ટો કરન્સી/**USDT** આપી બાકીના **રૂ. ૨૦, ૦૦, ૦૦૦/ - ના ક્રીપ્ટો કરન્સી/ USDT** ન આપી છેતરપીંડી કરેલ. જેમા ૧૦૦% રકમ બેંક એકાઉન્ટમાં ફ્રીઝ

- **ન્યુઝ પેપરમાં ફ્રેન્ડશીપ ક્લબના નામથી છોકરીઓ સાથે મુલાકાત કરો અને નાણા કમાવો એવી ટચુકડી જાહેરાત આપી છેતરપીંડી કરતી ગેંગનો પર્દાફાશ:**

  ન્યુઝ પેપરમાં કોમલ બ્યૂટી પાર્લરના નામે ટચુકડી જાહેરાત આપી એન.આર.આઇ. છોકરીઓ સાથે મુલાકાત કરો અને બે કલાક વાત કરવાની અને ખુશ રાખવાથી રૂ.૨૫,૦૦૦/- થી ૩૦,૦૦૦/- મળશે તેવી લોભામણી લલચામણી જાહેરાતો આપી છેતરપીંડી કરતી ગેંગના **કુલ- ૦૨ આરોપીઓને મહારાષ્ટ્રથી અટક કરેલ છે.**

સાયબર ક્રાઈમ

યુનિક કન્સ્ટ્રક્શનના બેંક એકાઉન્ટમાંથી ૧.૭૧ કરોડ રૂપિયા ગાયબ કર્યા હતા, બે નાઈજિરિયન સૂત્રધાર

ઓનલાઈન ઠગાઈ.. આંતરરાષ્ટ્રીય ગેંગ ઝડપાઈ

કમ્પ્યુટર હેક કરીને કે મેલ આઈડી-નેટબેંકિંગના પાસવર્ડ ચોરી કરોડોની ઉચાપત કરાતી, પાંચની ધરપકડ

આ ભેજાબાજો પકડાયા

આરોપીઓને બોગસ બિલિંગ અને છેતરપિંડી સહિતનો ગુનાઇત ઇતિહાસ

સાયબર માફિયાઓએ ગોઠવેલી ચેઇનની આ રીતે પોલીસને મળી કડી

એકાઉન્ટ હોલ્ડર આપવા, નાણાં વિડ્રોલ કરવા એજન્ટોને ૧થી ૧૦ ટકા કમિશન ચૂકવાતું

દેશની ૫૦થી વધુ હોસ્પિટલોની ફેક વેબસાઈટ બનાવી કિડની વેચાણની લોભામણી જાહેરાત મૂકી હતી

કિડનીના નામે ઠગાઈ કેસમાં આફ્રિકન ઝડપાયો

પર્દાફાશ નાનપુરાના યુવકને રૂ. ૪ કરોડમાં કિડની ખરીદવાનો ઝાંસો આપી ૧૪.૭૮ લાખ પડાવી લીધા હતા

આફ્રિકન ભેજાબાજ જુદીજુદી MOથી લોકોને ઓનલાઇન છેતરતો હતો

BCAના અભ્યાસ માટે ૨૦૦૮માં સ્ટુડન્ટ વિઝા પર આવ્યો

ઠગ ગેંગમાં બે નાઇજીરિયન પણ સામેલ

૨૦૧૧માં ફેક બોનોફાઇડ સર્ટિ બનાવતા પકડાયો હતો

૮ બેંકમાં એકાઉન્ટ, રૂ. ૧.૩૧ કરોડનું ટ્રાન્ઝેક્શન

પોલિસી છોડાવવાના ચાર્જિસને નામે ઠગાઈ કરતી દિલ્હીની ગેંગ ઝબ્બે ચઢી

| સુરત |

સુરત સાયબર ક્રાઈમે દીલ્હીમાં કોલ સેન્ટર ચલાવતાં ચારને ઝડપી લીધા હતા. આ ટોળકીએ નિવૃત બેન્ક મેનેજર અને તેના પરિવાર પાસે ઓન લાઈન ૭૦ પોલીસી લેવડાવી તેના નાણાં રિલીઝ કરવાના નામે ૪૨.૮૧ લાખ પડાવી લીધા હતા.

પોલીસ કમિશનર અજય તોમરે જણાવ્યું હતું કે ગત માર્ચ મહિનામાં દેના બેન્કનાં નિવૃત મેનેજરે સાયબર ક્રાઈમ સેલમાં છેતરપીંડીની ફરિયાદ નોંધાવી હતી. ૨૦૧૭થી તેમને ઈન્શયોરન્સ એજન્ટ તરીકે યુવતી અને યુવાનોના ફોન આવતા હતા. જંગી આવકની લાલચ આપતાં આ બેન્ક મેનેજરે પોતાના તથા પરિવારના નામે ૪૮.૩૬ લાખની કુલ ૭૦ પોલીસીઓ લીધી હતી. આ પોલીસીના નાણાં રિલીઝ કરવા જી.એસ.ટી. તથા વિવિધ ચાર્જીસના નામે ફોન કરી ૪૨.૮૧ લાખ રુપિયા પડાવી લીધી હતી. આ ટોળકી દીલ્હીના સાદરામાં કોલસેન્ટર ચલાવતી હોવાનું સાયબર ક્રાઈમની ટીમે વર્કઆઉટ કરી શોધી નાંખ્યું હતું અને ઉત્તર પ્રદેશના બદાયું જિલ્લામાં રહેતાં અબ્દુલ મન્નાન કય્યુમ ખાન, ઉમર સલીમ મીયાં, આકીબ અંસાર ખાન અને ઈરફાન અહમદ નિશાર અહમદની ધરપકડ કરી હતી.

સોશિયલ એન્જિનીયરીંગમાં ગઠિયાઓ માહેર

આઠથી ૧૨ ધોરણ ભણેલા ગઠિયાઓ છેતરપીંડી કરવા તમામ તર્કનો ઉપયોગ કરતા. જેને શિકાર બનાવવાનો હોય તેની તથા પરિવારની તમામ વિગતો ભેગી કરી લેતાં હતા. કોઇ પણ પોલીસી ઓનલાઇન લેવા કરતાં અધિકૃત કંપની તથા તેના કર્મચારી પાસે લેવાનો આગ્રહ કરવાની સાથે સાયબર જાગૃતિ માટે પોલીસે શરુ કરેલી સાયબર સંજીવનીની મદદ લેવા અજય તોમરે લોકોને અપીલ કરી હતી.

ડિસ્ટ્રિક્ટ કોર્ટની ક્લાર્ક સાથે ઓનલાઈન છેતરપિંડી કરનાર નેપાળી યુવતી ઝડપાઈ

| સુરત |

લોકડાઉનમાં વર્ક ફ્રોમ હોમ દરમિયાન બીજું કોઈ કામ મળી રહે તે માટે ઓનલાઈન સર્ચ દરમિયાન ઓનલાઈન રોકાણ કરવામાં નફાની લાલચ આપી ડિસ્ટ્રિક્ટ કોર્ટની ક્લાર્ક પાસેથી ૩.૫૭ લાખ પડાવી લેનાર પં.બંગાળના જલપાઈ ગુડીમાં રહેતી ૩૬ વર્ષીય નેપાળી મહિલાની ધરપકડ કરી હતી.

રામનગર ગવર્નમેન્ટ ક્વાર્ટર્સમાં રહેતા અને ડિસ્ટ્રિક્ટ કોર્ટમાં ક્લાર્ક તરીકે નોકરી કરતાં ૩૩ વર્ષીય પારૂલબેન પરમાર ગત કોરોના કાળ દરમિયાન માર્ચ મહિનામાં વર્ક ફ્રોમ હોમને લઈને ગૂગલ ઉપર તપાસ કરી રહ્યા હતા ત્યારે એક લીંક ભૂલથી ક્લીક થઈ જતાં તે તેમના મોબાઈલ ફોનમાં રજિસ્ટર થઈ ગઈ હતી. આ લીંક મોકલનાર વ્યક્તિએ પોતાની ઓળખ પેની તરીકે આપી હતી. યુનિલીવરના નામથી બનાવટી એપ્લિકેશન ડાઉનલોડ કરાવી હતી. ૨૧ દિવસમાં નફો થશે તેમ જણાવી મોટી રકમ રોકતાં તે ઉપાડવા માટે વધુ રકમનું રોકાણ કરવું પડશે તેમ જણાવી કુલ ૩.૫૭ લાખ ખંખેરી લીધા હતા.

આ ગુનાની તપાસ કરી રહેલા સાઈબર ક્રાઈમના ઈન્સ્પેક્ટર તરુણ ચૌધરીએ પં.બંગાળના જલપાઈ ગુડીના શુલ્કાપારામાં રેઈડ કરી ૩૬ વર્ષીય અનિતા સુબ્બાની ધરપકડ કરી હતી.

નવમું પાસ મહિલાએ ઊભા કરેલા ચાર એકાઉન્ટમાં સવા બે કરોડનું ટ્રાન્ઝેક્શન

પોલીસને આ ઠગના અલગ અલગ ચાર બેંક એકાઉન્ટ મળ્યા હતા. તે પશ્ચિમબંગાળના જ અન્ય ચાર વ્યક્તિના નામે હતા, પરંતુ તેમાં નંબર આ મહિલાનો હતો. આ ચાર એકાઉન્ટમાંથી દેશભરમાંથી ફ્રોડ કરીને મેળવાયેલાં સવા બે કરોડ કરતાં વધુનું ટ્રાન્ઝિક્શન મળી આવ્યું હતું. આ ઠગ માત્ર નવમું પાસ હતી. આ નાણાં કોની કોની પાસેથી છેતરપિંડી કરીને મળવ્યા તે જાણવા પોલીસે તેના સાત દિવસના રિમાન્ડ મેળવ્યા હતા.

ઓનલાઈન રમીના નામે લોકો પાસે ખાતું ખોલાવી તેના નાણાં, રૂપિયા ડબલ કરવાની સ્કીમમાં નાખી કૌભાંડ કરાયું

ચીની એપથી કરાયેલા 520 કરોડનાં કૌભાંડમાં સુરતના વેબડેવલપર અને ચાવાળો ઝડપાયા

વેસુના ચાવાળા વિજય વણઝારાના ખાતામાં 3 કરોડ જમા થયા હતા, બેંગ્લુરુ પોલીસે વિજયનું ખાતુ સિઝ કર્યું

પકડાયેલા આરોપીઓ.

કેવી રીતે ભેરવાયા

રોઝરપે થી કૌભાંડ બહાર આવ્યું

નવતર પ્રયોગ લોકોને જાગૃત કરવા પોલીસ કમિશનર અજય તોમરે સાઇબર સંજીવની એપ લોન્ચ કરી

સાઈબર ક્રાઈમથી બચવા ક્વિઝ કોમ્પિટિશન યોજાશે

સાત મહિનામાં જ સુરતીઓ સાથે 3.06 કરોડની છેતરપિંડી

સેલની સિદ્ધિઓ

દરેક રાજ્યમાં ગોઠવેલા નેટવર્કમાં કામ કરતા માણસો મારફતે ઠગાઈ

RBL બેન્કના ક્રેડિટ કાર્ડ ધારકો સાથે ઠગાઈ કરતી ગેંગનો સૂત્રધાર ઝારખંડથી ઝડપાયો

(પ્રતિનિધિ દ્વારા) સુરત, બુધવાર

સુરતના વેસુની એસ.ડી. જૈન સ્કુલના મહિલા એકાઉન્ટન્ટને આરબીએલ કંપનીના ક્રેડિટ કાર્ડ પર શોપીંગ વાઉચરની લાલચ આપી રૂ. ૨૧ હજારનું વીજ બીલ ભરવાના ગુનામાં કતારગામ પોલીસે ભાવનગરના પોલીસ પુત્ર સહિત ત્રણની ધરપકડ કર્યા બાદ હાથ ધરેલી તપાસમાં ઝારખંડના જામતારાથી ઓપરેટ થતા એક મોડયુલનો પર્દાફાશ થયો હતો. જેમાં ગેંગના સૂત્રધાર જીતેન્દ્ર ઉર્ફે રાહુલ મંડલને ઝડપીને ૬ મોબાઈલ ફોન અને

ધર્મેન્દ્રસિંહ ઝાલાના પુત્ર વિરભદ્રસિંહ (ઉ.વ.૨૯, રહે. બી/૧૧, ફ્લેટ નં.૧૨૮, જુની પોલીસ લાઈન, નવાપરા, ભાવનગર), ઓનલાઈન વસ્તુઓ વેચતા મેહુલ જવેરભાઈ કાકડીયા (ઉ.વ.૨૮, રહે. ઘર નં-.૪૦૧, જ્ઞાન પ્રવાહ એપાર્ટમેન્ટ, હરિદર્શનનો ખાડો, સિંગણપોર, કતારગામ, કતારગામ, સુરત. મૂળ રહે.મેથા પીપળીયા, તા.કુકાવાવ, જી. અમરેલી) અને બેકાર મિલન હરસુખભાઈ ચોવટીયા (ઉ.વ.૨૨, રહે.૯૪, હરીહરી સોસાયટી વિભાગ ૨, કતારગામ, સુરત. મૂળ રહે.જસાપર, તા.જામકંડોળા, જી.રાજકોટ) ની ધરપકડ કરી પુછપરછ કરતા આરબીએલ બેન્કના ક્રેડિટ કાર્ડ ધારકોને છેતરવાનું આખું મોડયુલ ઝારખંડના જામતારાનો જીતેન્દ્ર ઉર્ફે રાહુલ ટેકલાલ મંડલ (ઉ.વ.૨૫, રહે. ચામલીટી ગામ, જી. ગિરડીહ, ઝારખંડ) ઓપરેટ કરતો હોવાનો ખુલાસો થયો હતો.

મંગળવાર ૩ ઓગસ્ટ, ૨૦૨૧ — ગુજરાતમિત્ર તથા ગુજરાતદર્પણ, સુરત

ઓનલાઇન લલચામણીથી સાવધાન

હનીટ્રેપ.. યુવાનને મોત માટે મજબુર કરનાર ગેંગના સાગરિતની હરિયાણાથી ધરપકડ

આપઘાત કરતા પહેલા યુવાને આ ગેંગને ફોટા મોકલયા હોવા છતાં વધુ પાંચ હજાર માંગ્યા હતા

યુવતીનો પ્રિ-રેકોર્ડેડ વિડીયો મૂકતા

દેશભરમાં ફ્રોડ કર્યાની આશંકા

લોકોને જાગૃત કરવા ઓનલાઈન સાયબર અવેરનેસ પ્રોગ્રામ 'સાયબર સંજીવની'નું આયોજન

વર્ક ફ્રોમ હોમમાં સાયબર ક્રાઈમના કેસ બે ગણા વધી ગયા

વર્ષ-2021માં જાન્યુઆરીથી જુલાઈ સુધીમાં 203 કેસ નોંધાયા, સુરત પોલીસ દ્વારા વધતા સાયબર ફ્રોડમાં સાયબર ક્રાઈમ વેક્સિન અપાશે

સાયબર ક્રાઈમ પોલીસને મળેલી મોટી સફળતાઓ

ફ્લાઈંગ કલર્સ ડ્રોઈંગ સ્પર્ધાનું પણ આયોજન

છેલ્લાં ચાર વર્ષમાં થયેલા સાયબર ક્રાઈમના ગુના

વર્ષ	દાખલ ગુના (જુલાઈ સુધી)	દાખલ ગુના (ડિસે. સુધી)
2018	75	158
2019	144	238

લોકોને ઠગવા માટે આફ્રિકી નાગરિક પાસેથી ફેક વેબસાઈટ બનાવી કરોડોની છેતરપિંડી

કિડની ખરીદીના બહાને ઠગતો નાઈજીરિયન ઝડપાયો

કાયદાનો સકંજો | ત્રણ વર્ષથી ગેરકાયદે ભારતમાં રહેતા ગ્રેગરી યેરમડેની હરિયાણાથી ધરપકડ

યેરમેડે આફ્રિકન સાગરીતને ૨૦ ટકા કમિશન આપતો

■ સાયબર સંજીવની જનજાગૃત્તિ અભિયાનની સફળતા

African migrant caught for kidney racket

Times News Network

Surat: Cybercrime sleuths nabbed a 33-year-old illegal immigrant from Bangalore on Saturday who duped people through his fake kidney racket.

Accused Toty Dago Gregoire had cheated a businessman of Rs 14.78 lakh with the promise of getting him a client to sell his kidney. Police investigation revealed that Gregoire offered Rs 4 to Rs 7 crore for a kidney on his website advertisements.

Cops used a bait of Rs 4 crore to net the imposter who created a fake e-mail ID that looked similar to Reserve Bank of India's officer and also several websites of leading hospitals like Manipal Hospital, Apollo, Fortis, Max Super Speciality, Lilavati, Tata Memorial, among many others.

Accused in police custody

Police succeeded in freezing Rs 7.5 lakh in different bank accounts of the total fraud amount of Rs 14.78 lakh that the accused had transferred. They also seized a computer, a hard disk and four mobile phones from Gregoire who had come to India to study Bachelor of Computer Application in 2007. He went back home in 2010 but returned to India soon and never went back. His visa, however, expired and he is illegally staying in the country, police said.

According to police, accused had duped complainant Arbaz Rana, (25), a textile broker who later started selling used cars, between September and October 2020. Rana told the police that sans business for three years, he was in financial crisis and wanted to earn some quick money by selling off one kidney and get his sister married too.

"Rana borrowed money to pay for the fraud. He planned that he will repay the debt from the money received after selling the kidney," said Y A Gohil, assistant commissioner of police, cyber crime cell.

Examining eight bank accounts that Gregoire operated, police found transactions of Rs 1.31 crore.

"There could be many more accused involved in the crime but the African national is the mastermind. We request people to stay alert while entering in any dealings through the internet or over the phone," said city police commissioner Ajay Tomar.

Police found that Gregoire also created fake websites for forex trading and bitcoin investment besides offering jobs in airlines, agriculture, oil and gas, construction, dairy and courier delivery sectors in the UK, Canada and USA. He also created fake websites for exchanging old currency and also created separate websites offering Visas of different countries.

Gregoire also created four e-mail IDs that look similar to those of RBI officials.

સાયબર ક્રાઈમ: રાજ્યમાં રિકવરી - રિફંડમાં સુરત મોખરે

૧૪૭ સંસ્થા અને સાત લાખથી વધુ નાગરિકોએ ભાગ લીધો: પોલીસ કમિશનર તોમર

સાયબર ક્વિઝ

૧. નીચેના પૈકી કયો પાસવર્ડ સૌથી વધુ સુરક્ષિત છે?

(અ) Boat123 √ **(બ) WTh@5Z** (ક) 123456

૨. તમારે તમારા બધા ઓનલાઇન એકાઉન્ટસનો પાસવર્ડ એક સરખો રાખવો જોઈએ.?

(અ) હા √ **(બ) ના**

૩. તમારા સોશિયલ મીડિયા એકાઉન્ટસને પ્રાઇવેટ અને લોક રાખવું જોઇએ?

√ **(અ) હા** (બ) ના

૪. તમારા સોશિયલ મીડિયા એકાઉન્ટ્સમાં ટુ ફેક્ટર ઓથેન્ટિકેશન કાર્યરત રાખવું જોઇએ?

√ **(અ) હા** (બ) ના

૫. તમારે ઇ-મેઇલથી ખૂબ સંવેદનશીલ અને અંગત માહિતી મોકલવી જોઈએ?

(અ) હા √ **(બ) ના**

૬. તમારે કોઈ અજાણ્યા યુઝરને તમારો સંપર્ક કરવાથી રોકવા માટે તેને બ્લોક કરવો જોઈએ?

√ **(અ) હા** (બ) ના

૭. હંમેશા દરેક અજાણ્યા વીડિયો કોલ્સનો જવાબ આપવો જોઇએ? .

(અ) હા √ **(બ) ના**

૮. તમારે અનુચિત માહિતી, જાહેરાતો અને પોપ-અપ્સ પર ક્લિક કરવું જોઈએ?

(અ) હા √ **(બ) ના**

૯. સ્ક્રીન પર ગૂગલનું હોમપેજ લાવવા માટે, https://goagle.com સાચો URL સ્પેલિંગ છે?

(અ) હા √ **(બ) ના**

૧૦. હંમેશા કોઇપણ એપ્લિકેશન પ્લે સ્ટોર અથવા એપ સ્ટોર પરથી ડાઉનલોડ કરવી જોઇએ?

√ **(અ) હા** (બ) ના

૧૧. કોઈને પણ ઓટીપી / સીવીવી / પિનનંબર આપવો જોઇએ?

(અ) હા √ **(બ) ના**

૧૨. તમારે હંમેશાં કંપનીની ઓફિશીયલ વેબસાઇટ ઉપરથી જ કસ્ટમરકેર નંબર શોધવો જોઈએ?

√ **(અ) હા** (બ) ના

૧૩. સોશિયલ મીડિયા અન્યને અપમાનજનક / નુકસાનકારક ટિપ્પણીઓથી નુકસાન પહોંચાડવા માટે છે?

(અ) હા √ **(બ) ના**

૧૪. હંમેશા ઇ-મેઇલ મોકલનારનું ઇ-મેઇલ આઈડી ચકાસો, જે નામ દેખાય તેના પર વિશ્વાસ ના કરો.

√ **(અ) હા** (બ) ના

૧૫. ફક્ત જાણીતી અને વિશ્વસનીય વેબસાઇટ્સ પરથી જ વસ્તુઓ ખરીદવી/વેચવી જોઇએ?

√ **(અ) હા** (બ) ના

૧૬. પાસવર્ડ કોઇને પણ આપવાથી તમારા ઓનલાઇન એકાઉન્ટ્સ જોખમમાં મુકાઈ શકે અને તેનો દુરૂપયોગ થઈ શકે છે?

√ **(અ) હા** (બ) ના

૧૭. અજાણ્યા એસ.એમ.એસ/ઇ-મેઇલ દ્વારા મોકલવામાં આવેલ લિંક ઉપર ક્લીક કરવું જોઇએ ?

(અ) હા √ **(બ) ના**

૧૮. નાંણા મેળવવા માટે તમારે પિન / ઓટીપી / પાસવર્ડ આપવો પડે અથવા QR કોડ સ્કેન કરવો પડે?

(અ) હા √ **(બ) ના**

૧૯. જાહેર વાઇફાઇનો ઉપયોગ કરી બેંકિંગ ટ્રાન્ઝેક્શન કરવું જોઇએ?

(અ) હા √ **(બ) ના**

૨૦. તમારે સાયબર ક્રાઈમના કોઈપણ કિસ્સામાં પુરાવા માટે હંમેશા સ્ક્રીનશોટ લઇ સાચવવા જોઈએ?

√ **(અ) હા** (બ) ના

૨૧. તમારે તમારી કોઈપણ માહિતી ઓનલાઇન પોસ્ટ કરતા પહેલા હંમેશાં બે વાર વિચારવું જોઈએ?

√ **(અ) હા** (બ) ના

૨૨. સાયબર કેફે અથવા અજાણ્યા કોઇપણ ડિવાઇસનો ઉપયોગ કર્યાબાદ લોગઆઉટ થવું જોઇએ?

√ **(અ) હા** (બ) ના

૨૩. સોશિયલ મીડિયા પર આવેલ પોસ્ટને ખરાઇ કર્યા વગર ફોરવોર્ડ કરવી જોઇએ?

(અ) હા √ **(બ) ના**

૨૪. ઓનલાઇન તમામ એકાઉન્ટના પાસવર્ડ નિયમિત બદલતા રહેવું જોઇએ?

√ **(અ) હા** (બ) ના

૨૫. નોકરી મેળવવા ઓનલાઇન રજીસ્ટ્રેશન, ઇન્ટરવ્યુ માટે કોઇ કંપની નાણાની માંગણી કરે છે?

(અ) હા √ **(બ) ના**

૨૬. કોઇપણ એપ્લિકેશન ડાઉનલોડ કરતા સમયે એપ્લિકેશન વાપરવા જરૂરી હોય એટલી જ પરમિશન Allow કરવી જોઇએ?

√ **(અ) હા** (બ) ના

૨૭. જો આપના કોમ્પ્યુટરમાં રેન્સમવેર એટેક થયો હોય તો માંગેલ ખંડણીની રકમ ચુકવવી જોઇએ?

(અ) હા √ **(બ) ના**

૨૮. કોમ્પુટર /સર્વરના ડેટાનો નિયમિત બેક-અપ લેવો જોઇએ?

√ **(અ) હા** (બ) ના

૨૯. તમારી સાથે ઓનલાઇન કંઇ અજુગતુ થયુ હોય તો તુરંત કોઇ પુખ્ત વ્યક્તિને જાણ કરવી જોઇએ?

√ **(અ) હા** (બ) ના

૩૦. અજાણ્યા વ્યક્તિના કહેવાથી Any desk, Quick Support, Team Viewer જેવી એપ્લિકેશન ડાઉનલોડ કરવી જોઇએ?

(અ) હા √ **(બ) ના**

સુરત શહેર પોલીસ

તમારી સાથે, તમારા માટે

જો આપની સાથે ઓનલાઇન નાણાંકીય ફ્રોડ કે

અન્ય સાયબર ક્રાઇમ થાય છે તો તરત

24 કલાક કાર્યરત

સાયબર ક્રાઇમ હેલ્પ લાઇન નંબર ૧૯30 પર સંપર્ક કરો.

અથવા

ઓનલાઇન ફરિયાદ માટે વિઝિટ કરો

www.cybercrime.gov.in

સાયબર ક્રાઇમ પોલીસ સ્ટેશન, સુરત શહેરના નંબર પર સંપર્ક કરો.

સાઇબર ક્રાઇમ પોલીસ સ્ટેશન મોબાઈલ નંબર : +91 7069052555

સુરત સાઇબર ક્રાઇમ પોલીસ હેલ્પ લાઈન નંબર : +91 8160852285

સાઇબર ક્રાઇમ પોલીસ સ્ટેશન લેન્ડલાઇન નંબર : 0261-2653510

સુરત સાયબર મિત્ર ચેટ બોટ : +91 9328523417

Email:- polstn-cyber-sur@gujarat.gov.in

સંચાર સાથી પોર્ટલ :

સંચાર સાથી પોર્ટલ એ મોબાઈલ ગ્રાહકોને સશક્ત કરવા, તેમની સુરક્ષાને મજબૂત કરવા અને સરકારની નાગરિક કેન્દ્રિત પહેલો વિશે જાગૃતિ વધારવા માટે ટેલિકોમ્યુનિકેશન વિભાગની નાગરિક કેન્દ્રિત પહેલ છે. સંચાર સાથીમાં **ચક્ષુ, CEIR, TAFCOP, KYM, RICWIN, KYI** વગેરે જેવા વિવિધ મોડ્યુલો છે.

(૧) ચક્ષુ (Report Suspected Fraud Communication):

ચક્ષુ નાગરિકોને કોલ, SMS અથવા વ્હોટ્સએપ દ્વારા પ્રાપ્ત થયેલા શંકાસ્પદ સંદેશાવ્યવહાર જેવા કે નકલી ગ્રાહક સેવાઓ/ લોટરી ઓફર/લોન ઓફર/જોબ ઓફર અથવા KYC અપડેટ/ લોન વગેરેની જાણ/ફરિયાદ કરવાની સુવિધા આપે છે.

(૧) સૌ પ્રથમ સંચાર સાથી પોર્ટલ (https://sancharsaathi.gov.in/) પર જઈને હોમ પેજ પર **Citizen Centric Services** પર ક્લિક કરો.

(૨) હવે Report Suspected Fraud Communication પર ક્લિક કરી Continue for Reporting પર ક્લિક કરો.

(૩) Call, SMS, WhatsApp માંથી કોઇ એક ઓપ્શન સીલેક્ટ કરવો કે જે માધ્યમથી આપની સાથે છેતરપીંડી હોય. ત્યારબાદ કેટેગરી સીલેક્ટ કરી, સ્ક્રીનશોટ અટેચ કરો.

(૪) હવે છેતરપીંડીનો સમય, તારીખ તથા અન્ય માહિતી આપી, મોબાઇલ નંબર દાખલ કરી તથા OTP વેરિફાઇ કરાવી આપની ફરિયાદ દાખલ કરાવો.

(૨) CEIR (Central Equipment Identity Register):

CEIR મોડ્યુલ ખોવાયેલા/ચોરાયેલા મોબાઈલ ઉપકરણોને ટ્રેસ કરવાની સુવિધા આપે છે. આ ખોવાયેલા/ચોરાયેલા મોબાઈલ ઉપકરણોને બ્લોક કરવાની સુવિધા પણ આપે છે જેથી ભારતમાં ખોવાયેલા/ચોરાયેલા ઉપકરણોનો ઉપયોગ ન થઈ શકે. એકવાર મોબાઈલ ફોન મળી જાય તે પછી નાગરિકો દ્વારા તેના સામાન્ય ઉપયોગ માટે તેને પોર્ટલ પર અનબ્લોક કરવામાં આવી શકે છે.

(૧) સૌ પ્રથમ સંચાર સાથી પોર્ટલ (https://sancharsaathi.gov.in/) પર જઈને હોમ પેજ પર **Citizen Centric Services** પર ક્લિક કરો.

(૨) હવે **Block your Lost/Stolen Mobile** પર ક્લિક કરી, Block Lost/Stolen Mobile, Un-block Found Mobile, Check Request Status, Forgot Request ID માંથી જે લાગુ પડતો ઓપ્શન પર ક્લિક કરો.

(૩) Block Lost/Stolen Mobile ઓપ્શનમાં Device Information, Lost Information, Mobile Owner Personal Information તથા OTP વેરિફાઇ કરાવી Submit કરો.

(3) TAFCOP (Telecom Analytics for Fraud Management and Consumer Protection):

TAFCOP મોડ્યુલ મોબાઈલ સબસ્ક્રાઈબરને તેમના નામે લીધેલા મોબાઈલ કનેક્શનની સંખ્યા તપાસવાની સુવિધા આપે છે. જે મોબાઈલ કનેક્શન જરૂરી નથી અથવા ગ્રાહક દ્વારા લેવામાં આવ્યા નથી તે મોબાઈલ કનેક્શનની જાણ કરવાની પણ સુવિધા આપે છે.

(૧) સૌ પ્રથમ સંચાર સાથી પોર્ટલ (https://sancharsaathi.gov.in/) પર જઈને હોમ પેજ પર **Citizen Centric Services** પર ક્લિક કરો.

(૨) હવે **Know Your Mobile Connections** પર ક્લિક કરી, Mobile Number, Captcha, તથા OTP દાખલ કરી Login કરો.

(૩) મોબાઈલ સબસ્ક્રાઈબરને તેમના નામે લીધેલા મોબાઈલ કનેક્શનની સંખ્યા તથા મોબાઈલ નંબર બતાવશે, તેમજ મોબાઈલ નંબર સાથે Not My Number, Required, Not Required જેવા ઓપ્શનમાંથી લાગુ પડતો ઓપ્શન સીલેક્ટ કરવો.

(૪) KYM (Know Your Mobile):

KYM દ્વારા, તમે તમારા મોબાઇલ ઉપકરણને ખરીદતા પહેલા તેની માન્યતા ચકાસી શકો છો. મોબાઈલના પેકેજિંગ બોક્સ પર IMEI લખેલું હોય છે. તે મોબાઈલ બિલ/ઈનવોઈસ પર મળી શકે છે. તમારા મોબાઇલ પરથી તમે *#06# ડાયલ કરીને IMEI નંબર ચેક કરી શકો છો, IMEI નંબર મોબાઇલ સ્ક્રીન પર દેખાશે. જો મોબાઇલનું સ્ટેટસ બ્લેક-લિસ્ટેડ, ડુપ્લિકેટ અથવા પહેલેથી ઉપયોગમાં છે, તો કૃપા કરીને મોબાઇલ ખરીદવાનું ટાળો.

KYM નો ઉપયોગ 3 પદ્ધતિઓ દ્વારા થઈ શકે છે:

Web Portal દ્વારા, KYM એપ્લિકેશન દ્વારા અથવા SMS દ્વારા.

- SMS 14422 પર KYM<15 digit IMEI number> ટાઇપ કરી તમારા મોબાઇલમાંથી મોકલો.
- Web Portalમાં,

(૧) સૌ પ્રથમ સંચાર સાથી પોર્ટલ (https://sancharsaathi.gov.in/) પર જઈને હોમ પેજ પર **Citizen Centric Services** પર ક્લિક કરો.

(૨) હવે **Know Your Mobile Connections** પર ક્લિક કરી, Mobile Number, Captcha, તથા OTP દાખલ કરી Login કરો.

(૫) RICWIN (Report Incoming International Call With Indian Number):

RICWIN મોડ્યુલ નાગરિકોને સ્થાનિક ભારતીય નંબર (+91-xxxxxxxxxx) સાથે પ્રાપ્ત થતા આંતરરાષ્ટ્રીય કૉલ્સની જાણ કરવાની સુવિધા આપે છે.

(૧) સૌ પ્રથમ સંચાર સાથી પોર્ટલ (https://sancharsaathi.gov.in/) પર જઈને હોમ પેજ પર **Citizen Centric Services** પર ક્લિક કરો.

(૨) હવે **Report Incoming International Call With Indian Number** પર ક્લિક કરી, International call details, Captcha, તથા OTP વેરીફાઇ કરો.

- વૈકલ્પિક રીતે તમે 1963/1800110420 પર જાણ કરી શકો છો.

(૬) KYI (Know Your Wireline Internet Service Provider):

KYI મોડ્યુલ નાગરિકોને વાયરલાઇન ઇન્ટરનેટ સર્વિસ પ્રોવાઇડર (ISPs) ની વિગતો તપાસવાની સુવિધા આપે છે. મોડ્યુલ નાગરિકોને PIN કોડ, સરનામું અથવા ISPનું નામ દાખલ કરીને દેશની લંબાઈ અને પહોળાઈમાં કોઈપણ ISPની હાજરી શોધવા માટે સક્ષમ બનાવે છે.

(૧) સૌ પ્રથમ સંચાર સાથી પોર્ટલ (https://sancharsaathi.gov.in/) પર જઈને હોમ પેજ પર **Citizen Centric Services** પર ક્લિક કરો.

(૨) હવે Know Your Wireline Internet Service Provider પર ક્લિક કરો.

(૩) Search by PIN Code, Search by Address તથા Search by ISP Name માંથી એક ઓપ્શન સીલેક્ટ કરી સર્ચ કરો.

સાયબર પ્રતિજ્ઞા

૧. હું મારી વ્યક્તિગત વિગતો, જેવી કે મારું નામ, સરનામું, ફોન નંબર, ઇમેઇલ અને પાસવર્ડ અથવા શાળાના નામ આપવાનું ટાળીશ.

૨. હું જાણતો નથી અથવા વિશ્વાસ કરતો નથી, એવા અજાણ્યા લોકો તરફથી આવેલ ઇ-મેઇલ, ફાઇલો અથવા વેબ પૃષ્ઠોને ખોલીશ નહીં.

૩. હું ઓનલાઇન ક્યારેય કોઇને હેરાનગતી કે ખરાબ વર્તન કરીશ નહીં.

૪. હું ઓનલાઇન અજાણ્યા લોકોની ફ્રેન્ડ રીક્વેસ્ટ અથવા વીડિયો કોલ સ્વીકારીશ નહીં.

૫. જો કોઇ ઓનલાઇન મને ડરાવે, ધમકાવે, અસ્વસ્થ કરે અથવા રૂબરૂ મળવાનું કહે તો હું પુખ્ત વયના સંબંધીને અવશ્ય જણાવીશ.

૬. હું પોર્નોગ્રાફી વેબસાઇટ જોઇશ નહીં તેમજ ચાઇલ્ડ પોર્નોગ્રાફીને લગતો કોઇ વિડિયો/ઇમેજ ડાઉનલોડ કે ફોરવોર્ડ કરીશ નહીં.

૭. હું અજાણયા અનિચ્છનીય આવતા સંદેશા તથા કોલને બ્લોક કરીશ.

૮. હું યાદ રાખીશ કે પોસ્ટ કરેલી માહિતી ક્યારેય સંપુર્ણ દુર કરી શકાતી નથી.

૯. હું સોશિયલ મીડિયામાં કંઇપણ પોસ્ટ કરતાં પહેલાં બે વાર વિચારીશ.

૧૦. હું સોશિયલ મીડિયા સાઇટ્સ પર પ્રાયવેસી સેટિંગ્સનો ઉપયોગ કરીશ.

ડિસ્ક્લેમર: આ પુસ્તકમાં દર્શાવેલ ચિત્રો તથા કંપનીઓ તથા સર્વિસ પ્રોવાઇડરનાં નામ માત્ર અને માત્ર નાગરિકોને વિવિધ પ્રકારના સાયબર ક્રાઇમથી માહિતગાર કરવા અને જાગૃત કરવાની ભાવનાથી જ ઉપયોગ કરવામાં આવેલ છે.

આ બારકોડ સ્કેન કરો અને
સુરત શહેર પોલીસને ફોલો કરો...

@Cybersafesurat	@suratcitypolice	@SuratCityPolice	CP_SuratCity

સાયબર ક્રાઇમની માહિતી મેળવવા અને સાયબર ક્રાઇમથી બચવા

સુરત શહેર પોલીસના ફેસબુક, ઇન્સ્ટાગ્રામ, યુ-ટ્યુબ અને ટવીટર ઓફિશીયલ પેજને ફોલો, લાઇક અને સબસ્ક્રાઇબ કરો.