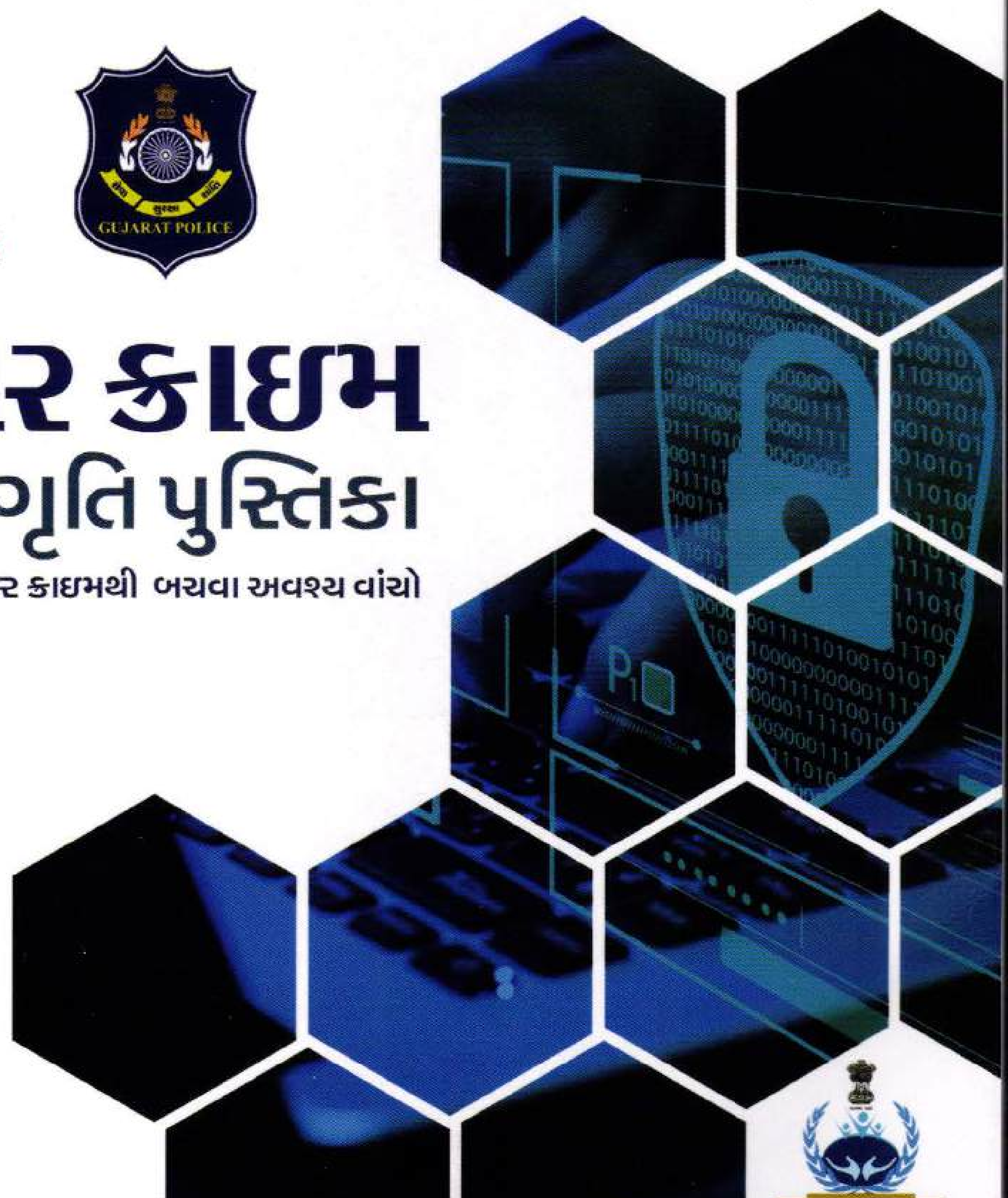
સ્ટેટ સાયબર ક્રાઇમ સેલ, સી.આઇ.ડી. ક્રાઇમ,
ગુજરાત રાજ્ય, ગાંધીનગર

દ્વારા પ્રસ્તુત

CID CRIME GUJARAT
Probing with Precision

GUJARAT POLICE



સાયબર ક્રાઇમ
જાગૃતિ પુસ્તિકા

સાયબર ક્રાઇમથી બચવા અવશ્ય વાંચો

Suraksha Setu Society
સુરક્ષા સેતુ સોસાયટીના
સૌજન્યથી

"નસીબ બચાવે એકવાર, સુરક્ષા બચાવે વારંવાર"

સાયબર ક્રાઇમની ફરિયાદ માટે **૧૯૩૦** | **NCCRP પોર્ટલ** **www.cybercrime.gov.in**

વધુ જાણકારી માટે @GujaratCyberCrimeCell અને @CyberGujarat ને ફોલો, લાઇક અને સબ્સ્ક્રાઇબ કરો.

CID CRIME GUJARAT
Probing with Precision

GUJARAT POLICE

જો આપની સાથે ઓનલાઇન નાણાંકીય ફ્રોડ કે અન્ય સાયબર ક્રાઇમ થાય છે તો તુરંત ૨૪ કલાક કાર્યરત સાયબર ક્રાઇમ ફરિયાદ નંબર અથવા ઓનલાઇન પોર્ટલ પર ફરિયાદ કરી શકો છો.

સાયબર ક્રાઇમ ફરિયાદ નંબર

૧૯૩૦

નેશનલ સાયબર ક્રાઇમ રીપોર્ટીંગ પોર્ટલ (NCCRP)

www.cybercrime.gov.in

અનુક્રમણિકા

માહિતી	પેજ નં.
- સાયબર ક્રાઇમ એટલે શું?	૧
- Digital Footprint	૨
- સાયબર ક્રાઇમ થવા પાછળના મુખ્ય કારણ	૩
- સાયબર ક્રાઇમના પ્રકારો	૪
- સાયબર ક્રાઇમ જાગૃતિ	૮
- ન્યુડ વિડિયો કોલીંગ ફ્રોડ	૯
- ઇન્સ્ટન્ટ લોન એપ ફ્રોડ	૧૦
- બનાવટી લિન્ક	૧૧
- ફેક કોલ	૧૨
- ઓનલાઇન સેલીંગ પ્લેટફોર્મ ફ્રોડ	૧૩
- સ્ક્રિન શેરીંગ એપ / રીમોટ એક્સેસ એપ ફ્રોડ	૧૪
- કસ્ટમર કેર ફ્રોડ	૧૫
- SIM સ્વેપ / SIM ક્લોનિંગ ફ્રોડ	૧૬
- અજાણી / અનવેરીફાઇડ મોબાઇલ એપ્લીકેશન ફ્રોડ	૧૭
- મહિલાઓ અને બાળકો માટે સાયબર સુરક્ષા	૧૮
- સોશીયલ મિડિયા સિક્યોરીટી	૧૯
- મોબાઇલ સિક્યોરીટી	૨૦
- ડિવાઇસ સિક્યોરિટી	૨૧
- સાયબર કાયદો	૨૨
- The Information Technology Act	૨૩
- ચાઇલ્ડ પોર્નોગ્રાફી	૨૪
- સાયબર ક્રાઇમ પોલીસ સ્ટેશન/સેલની યાદી અને સંપર્ક માહિતી	૨૫
- સાયબર ક્રાઇમથી બચવા માટે નાગરીકોને સુચન	૨૬

સાયબર વોલન્ટીયર યોજના

વધતા સાયબર ક્રાઇમને નાથવા માટે અને ગુજરાત પોલીસને મદદરૂપ થઇ શકે તે માટે ભારત સરકાર, ગૃહ વિભાગ દ્વારા સાયબર વોલન્ટીયર યોજના અમલમાં મુકવામાં આવેલ છે.

સાયબર વોલન્ટીયર બનવા માટે ઓનલાઇન

National Cyber Crime Reporting Portal (NCCRP)

www.cybercrime.gov.in

વેબસાઇટ પર લોગ ઓન કરી રજીસ્ટ્રેશન કરી સાયબર વોલન્ટીયર બની શકો છો.

સાયબર વોલન્ટીયર યોજના અંતર્ગત નીચે મુજબ ત્રણ પ્રકારના સાયબર વોલન્ટીયર બની શકાય છે.

- Cyber Volunteers for Unlawful Contents
- Cyber Awareness Promotor
- Cyber Expert

સાયબર ક્રાઇમ એટલે શું?

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

આજના ડિજીટલ યુગમાં ઇન્ટરનેટનો ઉપયોગ ફાયનાન્શીયલ, સોશીયલ તેમજ ઘણા બધા વ્યાપારીક હેતુઓ માટે કરવામાં આવે છે અને તમામ લોકો ઇન્ટરનેટથી સંકળાયેલ છે.

ઇન્ટરનેટની મદદથી આજના ડિજીટલ યુગમાં નાગરિકો સરળ રીતે ઘરે બેઠાજ ઓનલાઇન નાણાંકીય વ્યવહાર કરી શકે છે તેમજ દુનિયાની કોઇપણ વ્યક્તિ સાથે સંપર્ક કરી શકે છે જેથી કહી શકાય કે ઈન્ટરનેટે આપણું જીવન વધુ સુવિધાજનક બનાવ્યું છે.

ડિજીટલ યુગના ફાયદાઓ

ઝડપી કોમ્યુનિકેશન :

ઈન્ટરનેટનો સૌથી મહત્વનો ફાયદો ઝડપી કોમ્યુનિકેશન છે. આજના ડિજીટલ યુગમાં દુનિયાની કોઇ પણ વ્યક્તિ સાથે વિડીયો કોલીંગ, ઓડિયો કોલીંગ તેમજ એસ.એમ.એસ., ચેટ વગેરે તુરંત જ કરી શકીએ છીએ તે ખુબ જ સારી બાબત છે.

મનોરંજન :

ઇન્ટરનેટની મદદથી આપણે ઘરે બેઠા જ મનોરંજન પણ માણી શકીએ છીએ જેમ કે ફિલ્મો જોવા, નવા નવા વિડિયો જોવા, વેબ સીરીઝ વગેરે જેથી તેના માટે થિયેટર કે બીજે ક્યાય જવાની જરૂર પડતી નથી.

ઓનલાઇન શિક્ષણ :

આજના ડિજીટલ યુગમાં ઓનલાઇન ક્લાસના માધ્યમથી પણ ઓનલાઇન શિક્ષણ મેળવી શકાય છે.

ઈન્ટરનેટ વગર કંઈ જ નથી એટલે કે આજના જમાનામાં જે પણ કામ થઈ રહ્યું છે તે ઈન્ટરનેટ દ્વારા થઈ રહ્યું છે જે લોકો માટે ખૂબ જ સારું છે કારણ કે તેનાથી સમયની બચત થાય છે, નાણાંની બચત થાય છે, ઊર્જાની બચત થાય છે વગેરે.

ડિજીટલ યુગના ગેરફાયદાઓ

મહત્વના ડેટા અને માહિતીની ચોરી :

ઈન્ટરનેટના માધ્યમથી આજકાલ સાયબર ગઠીયાઓ અલગ અલગ ટેકનિકનો ઉપયોગ કરી તમને લાલચમાં લાવીને કે હેકર દ્વારા તમારી સીસ્ટમ હેક કરીને તમારી પર્સનલ માહિતી તેમજ ડેટા મેળવી લેતા હોય છે.

વાયરસ હુમલા:

કેટલાક વાયરસ પ્રોગ્રામ્સ ઇન્ટરનેટ દ્વારા આપણા કોમ્પ્યુટર પર મોકલવામાં આવે છે, જે આપણા કોમ્પ્યુટરને નુકસાન પહોંચાડે છે અને આપણા મહત્વપૂર્ણ ડેટાને બગાડે છે, જેના કારણે આપણે આપણો ડેટા ખોલી શકતા નથી. વાયરસ પ્રોગ્રામ્સ આપણાં કોમ્પ્યુટરનો મહત્વપૂર્ણ ડેટા કાઢી નાખે છે.

ઇન્ટરનેટનો ખોટો ઉપયોગ :

આજકાલ કેટલાક લોકો પછી તે બાળકો હોય કે વૃદ્ધ, ઈન્ટરનેટનો ખોટી રીતે ઉપયોગ કરવા લાગ્યા છે, જેનો અર્થ છે કે તેઓ ઈન્ટરનેટનો ઉપયોગ ખોટા વિડિયો જોવા માટે કરવા લાગ્યા છે, જેના કારણે લોકોની વિચારસરણી બદલાઈ જાય છે અને તેઓ ખોટા માર્ગે ભટકી જાય છે. કેટલાક લોકો કોઈને બ્લેકમેઈલ કરવાનું શરૂ કરી દે છે અને કોઈનો અંગત વિડિયો બનાવી ને ઈન્ટરનેટ પર અપલોડ કરવાની ભૂલ કરે છે.

Digital Foot Print

ડિજીટલ ફુટપ્રિન્ટ એટલે...

તમારા દ્વારા ઇન્ટરનેટના ઉપયોગથી કરવામાં આવતી ઓનલાઇન પ્રવૃત્તિ.

ઇન્ટરનેટનો ઉપયોગ કરતી વખતે ધ્યાન રાખો:

- શું શેર કરી રહ્યા છો?
- ક્યાં શેર કરી રહ્યા છો?
- કોને શેર કરી રહ્યા છો?

આપની ઇન્ટરનેટ એક્ટિવિટી
ક્યાંક ને ક્યાંક પુરાવો મુકતી જાય છે.

સાયબર ક્રાઇમ થવા પાછળના મુખ્ય કારણ

૧. માણસની માનસિકતા

ડર

નાગરિકો ઘણી વખત ડરમાં આવીને નાણાંકીય ચુકવણી કરી દેતા હોય છે અથવા તો અજાણી લિન્ક પર ક્લિક કરી માહિતી આપતા હોય છે અને છેતરપિંડીનો ભોગ બનતા હોય છે.

લાલચ

નાગરિકો ઘણી વખત ઇનામ, ઓફર વગેરે જેવા ખોટા મેસેજ કે લિન્કની લાલચમાં આવીને ખરાઇ કર્યા વગર ક્લિક કરી માહિતી તેમજ નાણાંની ચુકવણી કરી છેતરપિંડીનો ભોગ બને છે.

આળસ

નાગરિકો 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 છેતરપિંડીનો શિકાર બનતા હોય છે.

૨. ટેકનિકલ ભુલ

રેન્સમવેર/માલવેર

ટેકનિકલ ભુલ એટલે કે માણસની ભુલ સિવાય પણ આપણી સિસ્ટમમાં કોઇ ટેકનિકલ કારણોથી અચાનક રેન્સમવેર/માલવેર દાખલ થઇ જતા હોય છે જેના લીધે પણ સાયબર ક્રાઇમનો ભોગ બનતા હોઇએ છીએ.

હેકિંગ

હેકર દ્વારા ઘણી વખત આપણી જાણ બહાર સર્વરમાં દાખલ થઇ માહિતી મેળવી તેમજ ઇ-મેઇલ જેવા એકાઉન્ટની વિગતો મેળવી છેતરપિંડી આચરવામાં આવે છે.

સાયબર ક્રાઇમના પ્રકારો

- હેકિંગ
- ડેટા થેફ્ટ
- સાયબર બુલીંગ
- સોશીયલ મિડીયા ફ્રોડ
- ફાયનાન્સીયલ ફ્રોડ
- માલવેર / રેન્સમવેર

સાયબર બુલીંગ

- સોશીયલ મિડીયાની આજની દુનિયામાં, ભારતનો લગભગ દરેક યુવક વિવિધ પ્રકારના સોશીયલ મિડીયામાં 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 સોશીયલ મિડીયા 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 સોશીયલ મિડીયાને સોફ્ટવેર દ્વારા હેક કરે છે.
- હેકિંગ દ્વારા તમારા મોબાઇલ અને કોમ્પ્યુટરમાંથી તમારી પરવાનગી વગર ગુપ્ત માહિતી મેળવી છેતરપિંડી આચરે છે.

સોશીયલ મિડીયા ફ્રોડ

- આજકાલ લોકો Social Mediaનો ભરપુર ઉપયોગ કરી રહ્યા છે. કોઇ વેપાર માટે તો કોઇ મનોરંજન માટે, કોઇ ગપશપ કરવા માટે તો કોઇ નવા નવા મિત્રો બનાવવા માટે WhatsApp, Facebook, Instagram, Twitter, YouTube જેવા Social Media Platform વડે સતત એકબીજાના સંપર્કમાં રહેતા હોય છે.
- પરંતુ અહીં પણ તમારી સાથે છેતરપિંડી 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 વ્યકિતના ફોટો કે વિડિયો 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 વિડિયો અપલોડ કરવા, ટેગ અથવા શેર કરવુ પણ ગંભીર ગુનો બને છે

ડેટા થેફ્ટ

- એકદમ સરળ શબ્દોમાં કહીએ તો, કોઇપણ વ્યક્તિનો અંગત ડેટા, સંસ્થા, પ્રાઇવેટ કંપની કે સરકારી એકમોનો ડેટા વેબસાઇટ, કોમ્પ્યુટર, પેનડ્રાઇવ, ઇ-મેઇલ આઇ.ડી.ના માધ્યમથી ડિજીટલ ડેટા ચોરી કરવામાં આવે છે, જેને ડેટા થેફ્ટ કહેવાય છે.

માલવેર / રેન્સમવેર

- **Malware / Ransomware** એક પ્રકારનો દુષિત સોફ્ટવેર છે. જે આપમેળે જ ઇન્ટરનેટ અને ઇ-મેઈલથી તમારા કોમ્પ્યુટરમાં આવી જાય છે, જેના કારણે તમારા કોમ્પ્યુટરની તમામ ફાઇલ્સ **Encrypt** થઇ જાય છે.
- આ વાયરસ તમારી સિસ્ટમની અમુક ફાઇલ કે ફોલ્ડર, જે તમે રોજ યુઝ કરતા હોવ, તે શોધે છે.
- તે કોમ્પ્યુટરમાં ફ્રીક્વન્ટલી યુઝ્ડ 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 / Ransomware** વાયરસ.
- **Malware / Ransomware** વાયરસની કોઇ એક પેટર્ન નથી. તે અલગ-અલગ સર્વરથી, અલગ-અલગ લિન્કથી તમારી સીસ્ટમ, સર્વર કે ડિવાઇસ પર હાવી થઇ શકે છે.

ફાયનાન્સીયલ ફ્રોડ

- 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 ઉઠાંતરીના 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.

સાયબર ક્રાઇમ મોડસ ઓપરન્ડી

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

ન્યુડ વિડિયો કોલીંગ ફ્રોડ (Sextortion)

મોડસ ઓપરન્ડી

- સોશીયલ મિડિયા સાઇટ્સ જેમ કે ફેસબુકમાં 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 વિશ્વાસમાં લઇને તમારો વ્હોટ્સએપ નંબર માંગે છે કાતો એમનો વ્હોટ્સએપ નંબર આપે છે ત્યારબાદ વિડિયો કોલ કરવા માટે કહે છે, જેમાં સેક્સ વિડિયો કોલ માટે કહે છે.
- આમ કરવાથી ગઠીયાઓ વિડિયો રેકોર્ડીંગ એપ્લીકેશનથી વિડિયો રેકોર્ડ કરી વિડિયો બનાવે છે અને વાયરલ કરવાનું કહી નાણાંની માંગણી કરે છે.

સાવચેતી

- ક્યારેય નાણાંની ચુકવણી કરવી નહી અને આવી અજાણી પ્રોફાઇલની ફ્રેન્ડ રીક્વેસ્ટ એક્સેપ્ટ કરશો નહી અને વાતચીત કરવાનું ટાળો.

ઇન્સ્ટન્ટ લોન એપ ફ્રોડ

ઇન્સ્ટન્ટ લોન એપ દ્વારા ટુંકા સમયગાળા માટે લોન આપવાનું જણાવે છે.

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

ત્યારબાદ તમારા ફોટાનો દુરઉપયોગ કરી બદનામ કરી છેતરપીંડી આચરે છે.

સાવચેતી

- સાવચેતી:- આવી Insurance Loan એપ ખરાઈ કર્યા વગર ડાઉનલોડ કરવાનું ટાળો.
- તેમજ ફોટો અને કોન્ટેક્ટ Access Allow કરશો નહિ.

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 મિડિયા 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.
- નાગરિકોની બેન્ક ની તેમજ પર્સનલ માહિતી આવી બનાવટી લિન્ક દ્વારા ડેટા એન્ટ્રી હેઠળ મેળવી સાયબર ગઠીયાઓ આ માહિતીનો દુરઉપયોગ કરી છેતરપિંડી કરે છે.

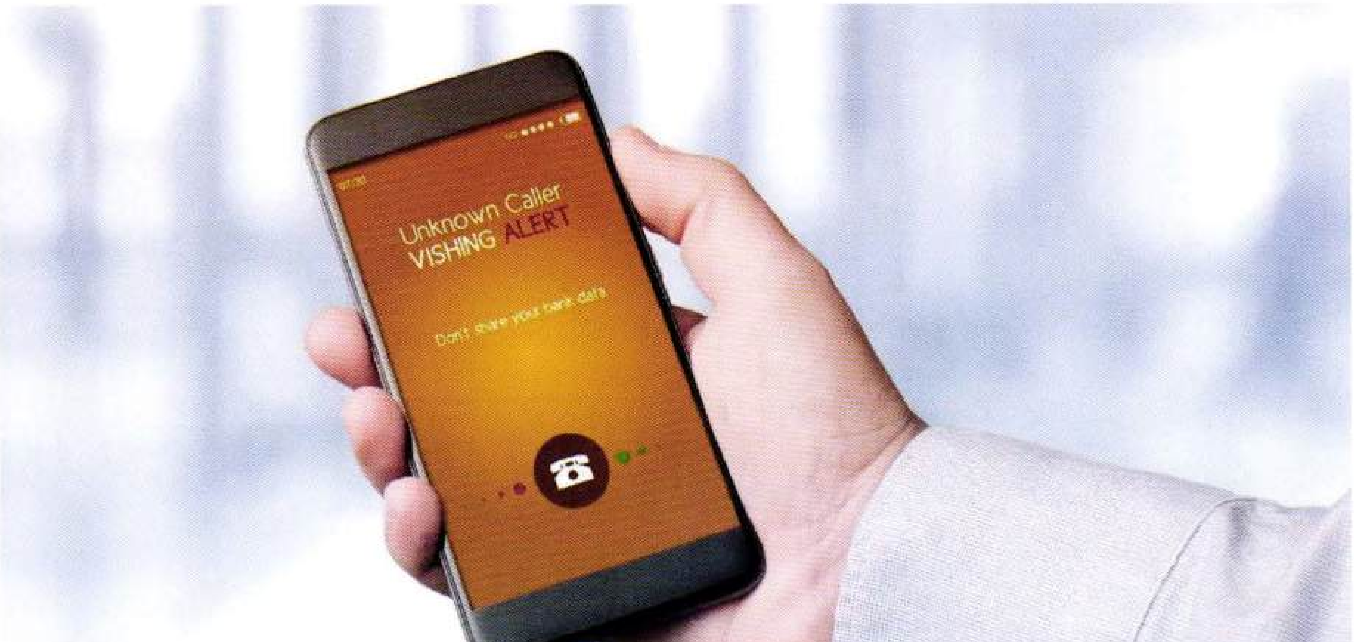
સાવચેતી

- અજાણી લિન્ક પર ક્લિક ન કરવું જોઈએ.
- વેબસાઇટની વિગતો ચકાસવા માટે ખાસ કાળજી લેવી.
- આવી લિન્ક ભુલથી પણ ઓપન થઇ જાય તો બેન્કની વિગત તેમજ પર્સનલ માહિતી દાખલ કરશો નહિ.

ફેક કોલ (Vishing Call)

મોડસ ઓપરન્ડી

- સાયબર ગઠીયાઓ ફોન કોલ કરી બનાવટી બેન્ક કર્મચારી/કંપની એક્ઝિક્યુટીવ/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 છેતરપિંડી કરે છે.



સાવચેતી

- બેન્ક / ફાઇનાન્સીયલ ઇન્સ્ટીટ્યુટ / કોઇપણ અધિકૃત સંસ્થા ક્યારેય બેન્કની વિગતો જેવી કે પાસવર્ડ, કાર્ડ ડિટેલ્સ, સી.વી.વી, ઓ.ટી.પી કે પિન માંગતી નથી.

મોડસ ઓપરન્ડી

- સાયબર ગઠીયા ઓનલાઇન સેલીંગ પ્લેટફોર્મ જેવા કે OLX, Facebook Market Place 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, Facebook Market Place 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 છેતરપિંડી કરે છે.
- OLX, Facebook Market Place જેવી એપ્લીકેશન પર સાયબર ગઠીયાઓ બાયર બની તમે ઉંચો ભાવ મુકો તો પણ તુરંત જ ખરીદ કરવા તૈયાર થઇ જાય છે અને તમને નાણાંની ચુકવણી કરવા માટે કોડ સ્કેન કરવા તેમજ રીક્વેસ્ટના માધ્યમનો ઉપયોગ કરી તમને નાણાં આપવાને બદલે મેળવી લેતા હોય છે.

સાવચેતી

- ઓનલાઈન પ્રોડક્ટ્સ માટે નાણાંકીય વ્યવહારો કરતી વખતે સાવચેત રહેવું જોઈએ.
- હંમેશા યાદ રાખો, નાણાં 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 નાણાં પ્રાપ્ત કરવાને બદલે નાણાં મોકલવાનું કામ કરી રહ્યા છો.

સ્ક્રિન શેરીંગ એપ / રીમોટ એક્સેસ એપ ફ્રોડ

મોડસ ઓપરન્ડી

- છેતરપિંડી કરનારા તમને સ્ક્રીન શેરિંગ એપ્સ **Team Viewer, AnyDesk** વગેરે 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 એપ્લિકેશન્સ ને એક્સેસ કરે છે અને તમારા ખાતામાંથી રૂપિયા 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.

મોડસ ઓપરન્ડી

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

સાવચેતી

- સર્ચ એન્જીનનો ઉપયોગ કરી કસ્ટમર 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 ઓ.ટી.પી. માટે ડુપ્લીકેટ સિમ કાર્ડનો ઉપયોગ કરતા હોય છે.
- સાયબર ગઠીયા નાગરિકોને કોલ કરી મોબાઇલ નેટવર્ક કર્મચારી બની નાગરિકોને 3G માંથી 4G કે 4G માંથી 5G કાર્ડ કન્વર્ટ કરવાના બહાને માહિતી મેળવી લે છે અને છેતરપિંડી આચરે છે.

સાવચેતી

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

મોડસ ઓપરન્ડી

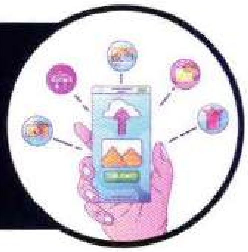
- સાયબર ગઠીયા અજાણી એપ્લિકેશન ડાઉનલોડ કરાવી તમારા મોબાઇલ ડિવાઇસ, લેપટોપ, કમ્પ્યુટરનું એક્સેસ મેળવી લે છે.
- આવી એપ્લિકેશનની લિન્ક સામાન્ય રીતે એસ.એમ.એસ./સોશીયલ મિડીયા/વ્હોટ્સએપ જેવી મેસેન્જર એપ દ્વારા મોકલવામાં આવે છે.
- આવી લિન્ક ઓરીજીનલ લિન્ક જેવી દેખાતી હોય છે પરંતુ તે માસ્ક કરેલ હોય છે અને ક્લિક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

સાવચેતી

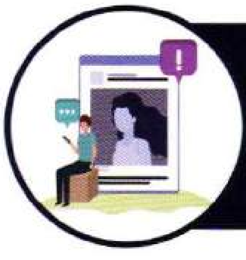
- અજાણી લિન્કને ક્લિક કરતા પહેલા વિચારો.
- અજાણી લિન્ક ઓપન કરી એપ્લિકેશન ડાઉનલોડ કરવી નહીં.

મહિલાઓ અને બાળકો માટે સાયબર સુરક્ષા

અજાણી ફ્રેન્ડ રિક્વેસ્ટ
એક્સેપ્ટ કરવાનું ટાળો.



તમારી અંગત માહિતી તેમજ
ફોટા વિડિયો શેર કરવાનું ટાળો.



સોશિયલ મિડીયા પર અજાણ્યા
વ્યક્તિ પર વિશ્વાસ ન કરો.

તમારી પોસ્ટ કરતી વખતે
તમારું લોકેશન શેર કરશો નહીં.

તમારા ઑનલાઇન મિત્રો ના અણધાર્યા
વર્તન અને પ્રવૃત્તિઓ અવગણશો નહીં.

બાળકોએ ધમકીભર્યા ઇ-મેઇલ, મેસેજ, પોસ્ટ
અથવા ટેક્સ્ટનો ક્યારેય જવાબ ન આપો અને
તુરંત માતા-પિતાને જાણ કરો.

ઓનલાઇન ગેમિંગ એપ્લિકેશનથી સાવચેત રહો
અને તેમાં ચેટ દરમ્યાન માહિતી આપવાનું ટાળો.

સોશીયલ મિડિયા સિક્યોરીટી (Social Media Security)

- આજના ડિજીટલ યુગમાં તમામ લોકો સોશીયલ મિડિયાથી સંકળાયેલ છે. સાયબર ગઠીયાઓ આવા પ્લેટફોર્મ દ્વારા છેતરપિંડી આચરે છે.
- જેથી સોશીયલ મિડિયા એકાઉન્ટને સિક્યોર રાખવુ ખુબ જ જરૂરી છે.

- ટુ ફેક્ટર ઓથેન્ટીકેશનનો ઉપયોગ કરો.
- પ્રોફાઇલ લોક રાખો.
- પ્રાઇવસી સેટીંગ્સ ઇનેબલ રાખો.
- પર્સનલ માહિતી શેર કરશો નહીં.
- પાસવર્ડ યુનિક અને સમયાંતરે બદલો.
- અજાણ્યા લોકોને મિત્ર બનાવશો નહીં.

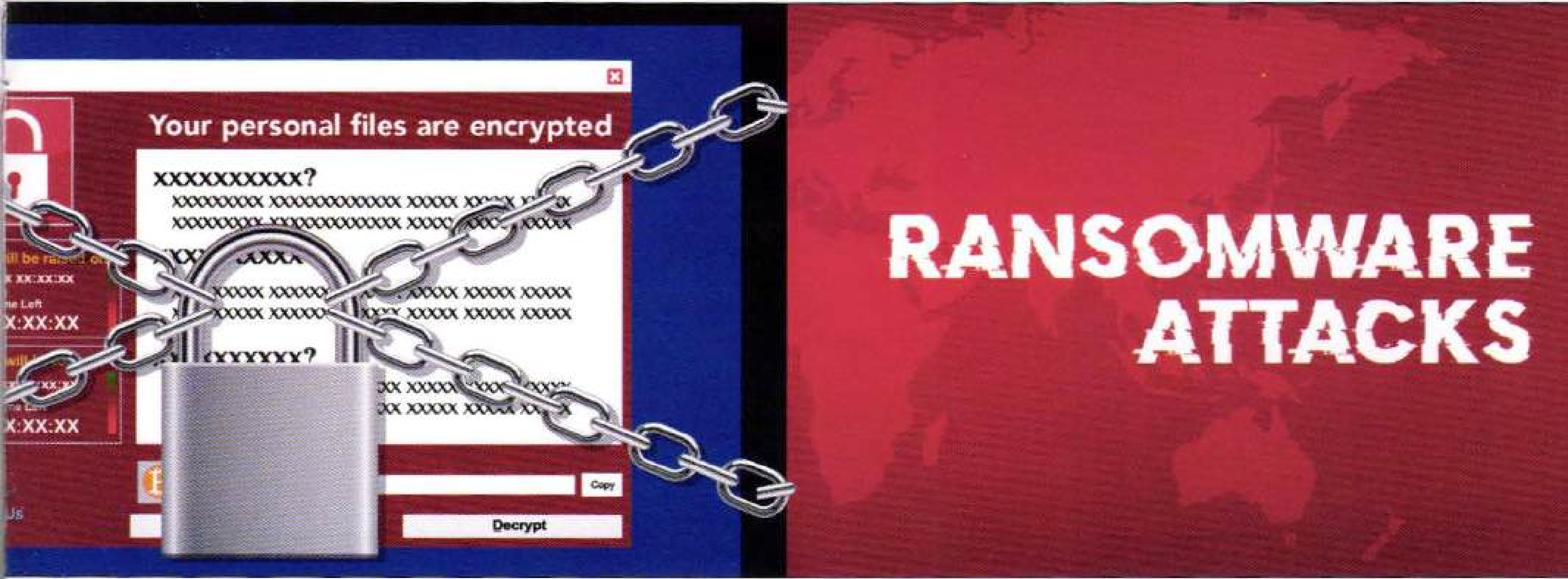
મોબાઇલ સિક્યોરીટી
(Mobile Security)

- સ્માર્ટ ડિવાઇસમાં વિવિધ પ્રકારના સિક્યોરીટી જોખમો છે જે મોબાઇલ ઉપકરણોને અસર કરે છે. જેથી મોબાઇલને નીચે મુજબ સિક્યોર રાખી શકાય.

- પાસવર્ડ પ્રોટેક્શન
- એન્ટી વાયરસ સોફ્ટવેર
- અપ-ટુ-ડેટ ઓપરેટીંગ સિસ્ટમ
- વિશ્વસનીય સોર્સ પરથી જ એપ્લિકેશન ડાઉનલોડ કરવી.
- રેગ્યુલર બેક અપ
- મોબાઇલ ગુમ થાય તો તમામ એકાઉન્ટના પાસવર્ડ બદલી લેવા જોઇએ.

ડિવાઇસ સિક્યોરિટી (Device Security)

- **Malware / Ransomware** એક પ્રકારનો દુષિત સોફ્ટવેર છે. જે આપમેળે જ ઇન્ટરનેટ અને ઇ-મેઈલથી તમારા કોમ્પ્યુટરમાં આવી જાય છે, જેના કારણે તમારા કોમ્પ્યુટરની તમામ ફાઇલ્સ **Encrypt** થઇ જાય છે.
- આ વાયરસ તમારી સિસ્ટમની અમુક ફાઇલ કે ફોલ્ડર, જે તમે રોજ યુઝ કરતા હોવ, તે શોધે છે.
- તે કોમ્પ્યુટરમાં ફ્રીક્વન્ટલી યુઝ્ડ 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 / Ransomware** વાયરસ.
- **Malware / Ransomware** વાયરસની કોઇ એક પેટર્ન નથી. તે અલગ-અલગ સર્વરથી, અલગ-અલગ લિન્કથી તમારી સીસ્ટમ, સર્વર કે ડિવાઇસ પર હાવી થઇ શકે છે.



સાયબર કાયદો (Cyber Law)

⊙ સાયબર કાયદો એ એવો કાયદો છે જે ઈન્ટરનેટ અને ઈન્ટરનેટ-સંબંધિત ટેક્નોલોજીને લાગુ પડે છે.

⊙ સાયબર કાયદો ઇન્ટરનેટનો ઉપયોગ કરતા લોકો ને કાનુની રક્ષણ પૂરું પાડે છે.

The Information Technology Act (2000)

Section 65 IT Act 2000:
કોમ્પ્યુટર સ્ત્રોત દસ્તાવેજો સાથે છેડછાડ.
ત્રણ વર્ષની જેલ / ૨ લાખ દંડ

Section 66 IT Act 2000:
કોમ્પ્યુટર સિસ્ટમ સાથે હેકિંગ.
ત્રણ વર્ષની જેલ / ૫ લાખ દંડ

Section 66B IT Act 2000:
ચોરાયેલ કોમ્પ્યુટર અથવા સંચાર ઉપકરણ પ્રાપ્ત કરવું.
ત્રણ વર્ષની જેલ / ૧ લાખ દંડ

Section 66C IT Act 2000:
અન્ય વ્યક્તિના પાસવર્ડનો ઉપયોગ કરવો.
ત્રણ વર્ષની જેલ / ૧ લાખ દંડ

Section 66E IT Act 2000:
અન્યના ખાનગી ફોટાઓ પ્રકાશિત કરવા.
ત્રણ વર્ષની જેલ / ૨ લાખ દંડ

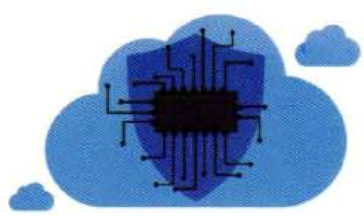
Section 67A IT Act 2000:
જાતીય કૃત્યો ધરાવતી છબીઓ પ્રકાશિત કરવી.
સાત વર્ષની જેલ / ૧ લાખ દંડ

Section 66F IT Act 2000:
સાયબર આતંકવાદના કૃત્યો.
આજીવન જેલ.

Section 70 IT Act 2000:
સંરક્ષિત સિસ્ટમની બિન-અધિકૃત ઍક્સેસ.
દસ વર્ષની જેલ

Section 72 IT Act 2000:
ગોપનીયતાનો ભંગ.
બે વર્ષની જેલ / ૧ લાખ દંડ

Section 73 IT Act 2000:
ઇલેક્ટ્રોનિક હસ્તાક્ષરનું પ્રમાણપત્ર ખોટું પ્રકાશિત કરી રહ્યું છે.
ત્રણ વર્ષની જેલ / ૨ લાખ દંડ



Information Technology Act, 2000

ચાઇલ્ડ પોર્નોગ્રાફી (Child Pornography)

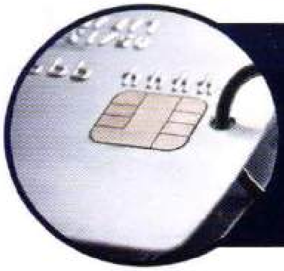
મોડસ ઓપરન્ડી

- **Section 67B** અંતર્ગત ચાઇલ્ડ પોર્નોગ્રાફી કાનુની અપરાધ છે.
- બાળકોના અશ્લીલ વિડીયો/ફોટોગ્રાફ સંબંધીત મટીરીયલ બનાવવુ, રાખવુ, ડાઉનલોડ, અપલોડ અને શેર કરવા કે કરાવવા તેમજ જોવા પણ ગંભીર અપરાધ બને છે.
- જેમાં પાંચ વર્ષ સુધીની કેદ અથવા રૂ.૧૦ લાખ સુધીના દંડની જોગવાઇ છે.
- ચાઇલ્ડ પોર્નોગ્રાફી બાબતે ગુજરાત પોલીસ દ્વારા સતત નજર રાખવામાં આવે છે અને તેમની વિરુધ્ધ સખ્ત કાર્યવાહી કરવામાં આવે છે.

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

સાયબર ક્રાઇમથી બચવા માટે નાગરીકોને સુચન
(Do's and Don'ts)



પીન નં., ઓ.ટી.પી., સી.વી.વી કે ક્યુ આર કોડ જેવી માહિતી અજાણ્યા વ્યક્તિને આપશો નહીં.

સોશીયલ મિડીયા પર અજાણ્યા વ્યક્તિનો વિડિયો કોલ કે ફ્રેન્ડ રીક્વેસ્ટ એક્સેપ્ટ કરતા પહેલા વિચારો.

કોઈ કાર્ડ, સીમ કાર્ડ વેલિડિટી, KYC રીન્યુ, ખાતુ ચાલુ/બંધ/એક્ટીવ વગેરે માટે ફોન કે મેસેજ પર જવાબ આપવાનું ટાળો.

પાસવર્ડને સુરક્ષીત રાખો, સમયસરે બદલો.

ફ્રી લોન, ફ્રી ઈન્ટરનેટ, ફ્રી ગીફ્ટ જેવી લાલચમાં ખરાઇ કર્યા વગર અજાણી લિન્ક ક્લિક કરશો નહીં.

સોશીયલ મિડીયા પર મિત્ર બની માહિતી કે રૂપિયાની માંગણી કરે તો આપશો નહીં.

લેટેસ્ટ સાયબર ક્રાઇમની માહિતી મેળવવા અને
સાયબર ક્રાઇમથી બચવા ગુજરાત સાયબર ક્રાઇમ સેલના
ફેસબુક, ઇન્સ્ટાગ્રામ, યુ ટ્યુબ અને ટ્વીટર ઓફીશીયલ પેજને
ફોલો, લાઇક અને સબ્સ્ક્રાઇબ કરો.

@GujaratCyberCrimeCell

@GujaratCyberCrimeCell

You Tube @GujaratCyberCrimeCell

@CyberGujarat

CID CRIME GUJARAT

Probing with Precision

GUJARAT POLICE

સ્ટેટ સાયબર ક્રાઇમ સેલ, સી.આઇ.ડી. ક્રાઇમ,
ગુજરાત રાજ્ય, ગાંધીનગર
દ્વારા પ્રસ્તુત

સાયબર ક્રાઇમની ફરિયાદ માટે **૧૯૩૦** | **NCCRP પોર્ટલ** **www.cybercrime.gov.in**

વધુ જાણકારી માટે ગુજરાત સાયબર ક્રાઇમ સેલના
સોશીયલ મિડીયા સાથે જોડાવવા આપેલ QR Code સ્કેન કરો

@GujaratCyberCrimeCell | @GujaratCyberCrimeCell | @GujaratCyberCrimeCell | @CyberGujarat