



# સાચબર સેફ ગર્લ



સાચબર ક્ષાઈમ ધ્રાન્ય, અમદાવાદ શહેર



## ડિસ્ક્લેમર

આ પુસ્તક સાયબર ક્રાઇમ બ્રાન્ચ, અમદાવાદ શહેર તરફથી નાગરિક અને ખાસ કરીને વિદ્યાર્થી – વિદ્યાર્થિનીઓને સરળતાથી ચિત્ર અને વાર્તાના માધ્યમથી વિવિધ પ્રકારના સાયબર ક્રાઇમથી માહિતગાર કરવા અને જાગૃત કરવાની ભાવનાથી તૈયાર કરવામાં આવેલ છે. આ પુસ્તકનો લાભ ગુજરાતની જનતાને મળે તે માટે ડૉ. અનંત પ્રભુ અને તેમની સાયબર સેફ ગર્લ ટીમની સ્વીકૃતિથી અને તેઓના સહયોગથી પ્રકાશિત કરવામાં આવેલ છે. વાર્તાઓ વધુ વાસ્તવિક લાગે તે હેતુથી ઘણીખરી કંપની તથા સર્વિસ પ્રોવાઇડરનાં નામ પણ રજૂ કરવામાં આવેલ છે, પરંતુ તેનો મતલબ એવો નથી કે, આ કંપનીઓ આ પ્રકારના ગુનાઓ સાથે સંકળાયેલ છે અથવા તેને ઉત્તેજન આપે છે. આ પુસ્તકમાં દર્શાવેલ તમામ વાર્તા તથા પાત્ર કાલ્પનિક છે, જે કોઈ ચોક્કસ વ્યક્તિ/ સમૂહ અથવા સમાજનું પ્રતિનિધિત્વ કરતાં નથી. આ પુસ્તકમાં દર્શાવેલ વાર્તાઓના પ્રકારે ઘણાખરા અંશે સાયબર ક્રાઇમ થાય છે. પરંતુ, હકીકતમાં સાયબર ક્રાઇમ અલગ પ્રકારે થાય તેની શક્યતાઓ નકારી શકાય નહીં. આ પુસ્તકના માધ્યમથી સાયબર ક્રાઇમથી આપના રક્ષણ માટે આપને આપવામાં આવેલ સલાહ – સૂચનથી આપ ઘણા અંશે સાયબર સેફ થઈ શકો છો.

## આભાર

અમારા સહયોગી, જેમની મદદ અને સહકારથી આ પુસ્તક તૈયાર કરવામાં આવ્યું છે.



ડૉ. અનંત પ્રભુ  
અને  
સાયબર સેફ ગર્લ ટીમ

unicef   
for every child

યુનિસેફ



રાષ્ટ્રીય રક્ષા  
યુનિવર્સિટી



સાયબર ક્રાઇમ બ્રાન્ચ, અમદાવાદ શહેર



## આભારસહ પરિચય

ડૉ. અનંત પ્રભુ, સાયબર સેફ ગર્લ પુસ્તકના લેખક છે. અત્રે રજૂ કરેલ આ પુસ્તક તેઓના દ્વારા રચિત પુસ્તક પર આધારિત છે. સદર પુસ્તકની સામગ્રી મહદંશે તેઓનું પુસ્તક Cyber Safe Girl ઉપર આધારિત છે. તેઓ તથા તેઓની ટીમ દ્વારા [www.cybersafegirl.com](http://www.cybersafegirl.com) વેબસાઇટ થકી તથા અન્ય માધ્યમથી સાયબર કાઇમ પ્રત્યે જાગૃતિ ફેલાવવા માટે પ્રયત્ન કરવામાં આવી રહ્યા છે. ડૉ. અનંત પ્રભુ લેખક, સોફ્ટવેર એન્જિનિયર, મોટીવેશનલ સ્પીકર તથા સાયબર સિક્યોરિટી નિષ્ણાંત છે. હાલમાં તેઓ ડિજિટલ ફોરેન્સિક્સમાં પ્રોફેસર તથા મુખ્ય તપાસ અધિકારી, સહ્યાદ્રી કોલેજ ઓફ એન્જિનિયરિંગ એન્ડ મેનેજમેન્ટમાં સાયબર સિક્યોરિટી સી.ઓ.ઈ. અને સ્યોરપાસ એકેડેમી ખાતે ડાયરેક્ટર તરીકે ફરજ બજાવે છે. આ ઉપરાંત તેઓ કર્ણાટક ન્યાયિક એકેડેમી અને કર્ણાટક પોલીસ એકેડેમી ખાતે સાયબર કાઇમ સંબંધિત કાયદા અને સાયબર સિક્યોરિટી સંબંધિત તાલીમ આપે છે. ઈન્ડિયા ટુડે મેગેઝિન દ્વારા વર્ષ ૨૦૧૯માં પ્રસિદ્ધ “Unsung Heroes of India” યાદીમાં તેઓ સ્થાન પામેલ છે. તેઓની વેબસાઇટ [www.cybersafegirl.com](http://www.cybersafegirl.com)નો લાભ લેવા આપને અનુરોધ છે.

સાયબર સેફ ગર્લ

---



## શુભેચ્છા સંદેશ

છેલ્લા દોઢ દાયકામાં ટેકનોલોજીનો વ્યાપ અને વહેવાર તેજ ગતિથી વધી રહ્યો છે. આંતરરાષ્ટ્રીય સ્તરે અને વિશ્વકક્ષાએ ગુજરાત રાજ્યે, ત્રોથ એન્જિન અને Role Model State તરીકે પોતાની આગવી ઓળખ ઊભી કરી છે. ગર્વની બાબત છે કે આદરણીય વડાપ્રધાન શ્રી નરેન્દ્રભાઈ મોદીના Vision સાથે ગુજરાતને આ માન અને ગૌરવ પ્રાપ્ત થયાં છે. પરિણામો સર્જનારી બની છે ત્યારે Cyber Crimeને વહેલાસર નાથવો એ પોલીસતંત્રની જવાબદારીપૂર્ણ પ્રતિબદ્ધતા બને છે. Cyber સુવિધાની દૂરુપયોગિતાથી જાહેર જનતાને અવગત રાખી, સુરક્ષિત રાખવા અમદાવાદ શહેર સાયબર ક્રાઈમ બ્રાન્ચ દ્વારા. સાઈબર સેફ મિશન અંતર્ગત સાઈબર સેફ ગર્લ પુસ્તિકા તૈયાર કરાઈ છે.

સાયબર ગુનાખોરો સામે લાલ આંખ રાખી, પ્રજાની સુખાકારી અને સલામતી માટે સરકારની પ્રતિબદ્ધતાને વ્યક્ત કરતી આ ઉમદા પહેલ માટે, સાઈબર ક્રાઈમ બ્રાન્ચ અને ગૃહવિભાગને શુભેચ્છા સહ અભિનંદન પાઠવું છું.

(ભૂપેન્દ્ર પટેલ)  
મુખ્યમંત્રી,  
ગુજરાત રાજ્ય

સાયબર સેફ ગર્લ

---





## શુભેચ્છા સંદેશ

આપણું ગુજરાત આજે જ્યારે વિકાસની કેડીએ અવિરત હરણફાળ ભરી રહ્યું છે, ત્યારે વિકાસ તરફી ગુજરાતની આ આગેકૂચમાં રાજ્યમાં પ્રવર્તમાન શાંતિ અને સલામતી એક અગત્યનું પરિબળ રહ્યું છે, જે એક નિર્વિવાદિત સત્ય છે.

પ્રવર્તમાન સમયમાં ગુજરાતસહિત સમગ્ર વિશ્વમાં એક તરફ ઈન્ટરનેટના વપરાશમાં ખૂબ જ મોટા પ્રમાણમાં વધારો થઈ રહ્યો છે, ત્યારે તેની સાથે સાથે, સાચબર કાઈમને લગતા ગુનાઓ વધી રહ્યાં છે. આથી ગુજરાતની પ્રજાની આર્થિક સુખાકારીની જાળવણી માટે સાચબર કાઈમને લગતા ગુનાઓ અટકાવવાની વિશેષ જવાબદારી ગુજરાત પોલીસના શિરે છે.

રાજ્ય સરકાર દ્વારા રાજ્યમાં સાચબર ગુનાઓ થતા અટકાવવા તેમજ થયેલ ગુનાઓના ત્વરિત નિવારણ માટે સાચબર કાઈમ પોલીસ સ્ટેશનોની રચના કરવામાં આવેલ છે. સાચબર કાઈમ વિભાગ દ્વારા જે અથાગ પ્રયત્નો થઈ રહ્યા છે, તેને કારણે પ્રજાનો પોલીસ તરફનો વિશ્વાસ વધતો જાય છે, તે બદલ ગુજરાત પોલીસની સમગ્ર ટીમ અભિનંદનને પાત્ર છે.

(હર્ષ સંઘવી)

ગૃહ રાજ્ય મંત્રી,  
ગુજરાત રાજ્ય

સાયબર સેફ ગર્લ

---



## શુભેચ્છા સંદેશ

આધુનિક સમયમાં સમગ્ર વિશ્વમાં ડિજિટલ યુગનો આરંભ થઈ ચૂકેલ છે. આવા સમયમાં ગુજરાત રાજ્ય પોલીસની કામગીરીમાં આધુનિકરણ અને innovation ની આવશ્યકતા છે. ટેકનોલોજીના દુરુપયોગના લીધે રાજ્યના નાગરિકોને સામાજિક અને આર્થિક નુકસાન ન થાય તથા નાગરિકો સુરક્ષા અનુભવે તે માટે સાયબર ક્રાઈમ પ્રાન્થ, અમદાવાદ શહેર દ્વારા તૈયાર કરવામાં આવેલ પુસ્તક, “સાયબર સેફ ગર્લ” થકી સાયબર ક્રાઈમ તથા સાયબર સુરક્ષા બાબતે નાગરિકોમાં જાગૃકતા કેળવવાનો ઉત્કૃષ્ટ પ્રયત્ન કરવામાં આવ્યો છે, જે ખૂબજ આપકારદાયક છે.

સાયબર ક્રાઈમ પ્રાન્થ, અમદાવાદ શહેરના આ પ્રયત્ન સફળ રહે તથા તેઓનો ધ્યેય સિદ્ધ થાય તેવી હું શુભકામનાઓ અર્પું છું.

(ડૉ. સંજય કુમાર ગુપ્તા)  
અધિક મુખ્ય સચિવશ્રી,

ગૃહ વિભાગ, ગુજરાત રાજ્ય

સાયબર સેફ ગર્લ

---



## શુભેચ્છા સંદેશ

સેવા, સુરક્ષા, શાંતિ જેની નેમ છે; કાયદો અને વ્યવસ્થા જેની જવાબદારી છે, એ ગુજરાત પોલીસ. વર્તમાન સમયમાં કાયદો અને વ્યવસ્થાની જાળવણીમાં ગુજરાત પોલીસે નવતર અભિગમ અપનાવ્યો છે. ગુનાખોરી અટકાવવા માટે રાજ્ય પોલીસ ટેકનોલોજીથી સુસજ્જ બની છે.

ટેકનોલોજીનો ઉપયોગ હાલમાં બહોળા પ્રમાણમાં વધી રહ્યો છે. જેમ જેમ સ્માર્ટ મોબાઇલ ફોન, ઇલેક્ટ્રોનિક્સ સંસાધનો તથા સોશિયલ મીડિયાનો ઉપયોગ વધી રહ્યો છે તેમ તેમ સાચબર કાઈમમાં પણ વધારો જોવા મળી રહ્યો છે. આ પ્રકારના સાચબર કાઈમને લગતા ગુનાઓને નાથવા માટે સાચબર કાઈમ ધ્રાન્ય, અમદાવાદ શહેર દ્વારા આ ખાસ પહેલ કરવામાં આવી છે, જેને હું આવકારું છું.

ગુજરાતની પ્રજાને નમ્ર અપીલ છે કે, તમે કોઈ પણ પ્રકારના સાચબર કાઈમનો ભોગ ના બનો તે સારુ આ ખાસ પહેલમાં જોડાશો અને પોતાને સક્ષમ બનાવશો.

જય હિન્દ.

(આશીષ ભાટિયા)

પોલીસ મહાનિદેશક અને  
મુખ્ય પોલીસ અધિકારીશ્રી,  
ગુજરાત રાજ્ય

સાયબર સેફ ગર્લ

---



## શુભેચ્છા સંદેશ

આજના ટેકનોલોજીના યુગમાં નાગરિકો ઓનલાઇન શોપિંગ, રિચાર્જ, નાણાંની ચુકવણી, ઈ-મિટિંગ, વેબીનાર જેવી ડિજિટલ સેવાનો લાભ લઈ રહ્યાં છે. કેટલાક સાયબર અપરાધીઓ દ્વારા આ જ ટેકનોલોજીનો દુરુપયોગ કરી લોકો સાથે છેતરપિંડી કરી માનસિક, શારીરિક, આર્થિક નુકસાન પહોંચાડવામાં આવી રહ્યું છે.

દિન-પ્રતિદિન સાયબર ક્રાઇમમાં વધારો થઈ રહ્યો છે ત્યારે નાગરિકોએ સાયબર ગુનાઓથી બચવા તકેદારી રાખવી અને આવા ગુનાનો ભોગ ન બને તે અંગે સાવધાની રાખવી જરૂરી છે. આપણી જ લાલચ, નિષ્કાળજી અને ઉતાવળને કારણે સાયબર ગુનાઓ વધે છે. સાયબર ગુનાઓ બનતા અટકે તે માટે નાગરિકોમાં જાગૃકતા કેળવવી જરૂરી છે. જેના માટે પુસ્તિકા ખૂબ જ ઉપયોગી નીવડે તેવી સંપૂર્ણ ખાતરી સાથે સાયબર ક્રાઇમ પ્રાન્થ, અમદાવાદ શહેરને આ ઉમદા કાર્ય માટે શુભેચ્છાઓ પાઠવું છું.

(સંજય શ્રીવાસ્તવ)  
પોલીસ કમિશનર  
અમદાવાદ શહેર

સાયબર સેફ ગર્લ

---





## શુભેચ્છા સંદેશ

આજના ટેકનોલોજીના યુગમાં આંગળીના ટેરવે બનતા અપરાધ એટલે સાચબર કાઈમ. ટેકનોલોજીના દુરુપયોગના લીધે રાજ્યના નાગરિકોને સામાજિક અને આર્થિક નુકસાન ન થાય તથા નાગરિકો પોતે સાચબર કાઈમનો ભોગ ન બને તે માટેનું શ્રેષ્ઠ આચરણ કરે તે માટે “સાચબર સેફ ગર્લ” પુસ્તિકા ખૂબ જ ઉપયોગી થશે.

આ પુસ્તક થકી નાગરિકોમાં વધુને વધુ જાગૃતિ કેળવી શકાય તથા વધુને વધુ લોકો સુધી આ પુસ્તક થકી પહોંચી શકાય તેવી શ્રી અમિત વસાવા, નાયબ પોલીસ કમિશનર, સાચબર કાઈમ વ્રાન્ચ, અમદાવાદ શહેર તથા તેમની ટીમને શુભકામનાઓ આપું છું.

જય હિંદ.

(પ્રેમ વીર સિંહ)

અધિક પોલીસ કમિશનર, કાઈમ

અમદાવાદ શહેર

સાચબર સેફ ગર્લ

---



## પ્રસ્તાવના

“સાયબર ક્રાઈમ” આજના ટેકનોલોજીના યુગમાં ખૂબ જ ઝડપથી વધી રહ્યો છે, આથી નાગરિકોએ સાયબર ગુનાઓથી બચવા કેવા પ્રકારની તકેદારી રાખવી અને આવા ગુનાનો ભોગ ન બને તે અંગે ડૉ. અનંત પ્રભુ અને સાયબર સેફ ગર્લ ટીમના સહયોગથી નાગરિકોમાં જાગૃકતા કેળવવા માટે તૈયાર કરેલ “સાયબર સેફ ગર્લ” પુસ્તિકા રજૂ કરતા હું અત્યંત હર્ષની લાગણી અનુભવું છું.

આ પુસ્તિકા દ્વારા રોજબરોજ બનતા સામાન્યથી લઈને મોટા સાયબર ક્રાઈમની ચિત્રસહ રજૂઆત કરવામાં આવેલ છે, આથી તમામ નાગરિકો તેને સરળ રીતે સમજી શકે. આ પુસ્તિકા તૈયાર કરવામાં મદદરૂપ રહેલા સાયબર આશ્વસ્ત પ્રોજેક્ટની ટીમના દરેક અધિકારી/ કર્મચારીને હું બિરદાવું છું.

જય હિંદ.

  
(અમિત વસાવા)

નાયબ પોલીસ કમિશનર,  
સાયબર ક્રાઈમ વ્રાન્ચ,  
અમદાવાદ શહેર

સાયબર સેફ ગર્લ

---

## અનુક્રમણિકા

કાયદાકીય માહિતી.....	૦૧
૧. મોબાઇલ રિચાર્જની દુકાન.....	૦૭
૨. ડેબિટ કાર્ડ કલોનિંગ.....	૦૯
૩. કી લોગર.....	૧૧
૪. મેસેજ સ્પૂફિંગ.....	૧૩
૫. કોલ સ્પૂફિંગ.....	૧૫
૬. રેન્સમવેર.....	૧૭
૭. સાચબર સ્ટોકિંગ.....	૧૯
૮. ફોટો મોર્ફિંગ.....	૨૧
૯. પ્રોફાઇલ હેકિંગ.....	૨૩
૧૦. ઓનલાઇન ગેમ્સ.....	૨૫
૧૧. જોબ ફ્રોડ.....	૨૭
૧૨. ડીપ ફેક.....	૨૯
૧૩. ડેટિંગ વેબસાઇટ.....	૩૧
૧૪. કેમેરા હેકિંગ.....	૩૩
૧૫. સોશિયલ ટ્રોલિંગ.....	૩૫
૧૬. પોન્ઝી સ્કીમ.....	૩૭
૧૭. મેટ્રીમોનીયલ વેબસાઇટ ફ્રોડ.....	૩૯
૧૮. મોબાઇલ રિપેર શોપ.....	૪૧
૧૯. ફેક રિવ્યુઝ.....	૪૩
૨૦. ફેક પ્રોફાઇલ અને સેક્સ્ટોર્શન.....	૪૫
૨૧. સાચબર ગીઢ.....	૪૭
૨૨. મોબાઇલ એપ્સ .....	૪૯
૨૩. ચાર્જિંગ પોઇન્ટ હેક.....	૫૧

૨૪.	વાઈફાઈ હેક.....	૫૩
૨૫.	ઓનલાઈન કન્ટ્રિપાઈ ફેલાવવો.....	૫૫
૨૬.	હની ટ્રેપ.....	૫૭
૨૭.	QR કોડ.....	૫૯
૨૮.	RFID ક્લોનિંગ.....	૬૧
૨૯.	ડ્રોન સર્વેક્ષણ.....	૬૩
૩૦.	ગુગલ સર્ચ.....	૬૫
૩૧.	IDN હોમોગ્રાફ એટેક.....	૬૭
૩૨.	સ્કેચકાર્ડ.....	૬૯
૩૩.	સીમ સ્વેપ.....	૭૧
૩૪.	ફિષ્ટો જેકિંગ.....	૭૩
૩૫.	વીડિયો કોનફરન્સ.....	૭૫
૩૬.	મોબાઈલ ફોન અને નાનાં બાળકો.....	૭૭
૩૭.	સ્માર્ટ હોમ્સ.....	૭૯
૩૮.	માઈક્રો લોન્સ.....	૮૧
૩૯.	બ્લૂ સ્નાર્ફિંગ.....	૮૩
૪૦.	ખોવાયેલો મોબાઈલ ફોન.....	૮૫

સાયબર સેફ ગર્લ

---

## કાયદાકીય માહિતી

અત્રે દર્શાવેલ વિવિધ વાર્તા ચિત્રો સાથે સંલગ્ન સાચબર ફોડ તથા અન્ય સાચબર ગુનાઓને લગતી કાયદાકીય જોગવાઈ અને લાગુ પડતી કલમને લગતી માહિતી નીચે મુજબ છે.

### લાગુ પડતી ઈ.પી.કો. કલમો

- ૧ ઈ.પી.કો. કલમ ૩૪ : જુદી જુદી વ્યક્તિઓ દ્વારા એકસમાન ઈરાદો પાર પાડવા કરવામાં આવેલ કૃત્ય
- ૨ ઈ.પી.કો. કલમ ૧૦૯ : ગુનાહિત કૃત્ય માટે સહાય કરવા બદલ સજા
- ૩ ઈ.પી.કો. કલમ ૧૧૪ : ગુનો આચરવામાં આવે ત્યારે સહાયકર્તાની હાજરી
- ૪ ઈ.પી.કો. કલમ ૧૨૦ : ગુનાહિત કાવતરા બદલ સજા (બી)
- ૫ ઈ.પી.કો. કલમ ૨૯૨ : અશ્લીલ પુસ્તકો વગેરેનું વેચાણ (જો હાર્ડકોપીમાં હોય તો)
- ૬ ઈ.પી.કો. કલમ ૨૯૩ : તરૂણ વ્યક્તિને અશ્લીલ વસ્તુઓ વેચવા બાબત
- ૭ ઈ.પી.કો. કલમ ૨૯૯ : ગુનાહિત માનવ વધ
- ૮ ઈ.પી.કો. કલમ ૩૦૫ : બાળક અથવા પાગલ વ્યક્તિને આત્મહત્યા માટે દુષ્પ્રેરણ
- ૯ ઈ.પી.કો. કલમ ૩૦૬ : આત્મહત્યા માટે ઉશ્કેરણી કરવી.
- ૧૦ ઈ.પી.કો. કલમ ૩૨૧ : જાણીજોઈને અન્યને વ્યથિત કરવું.



- ૧૧ ઈ.પી.કો. કલમ ૩૩૫ : ઉશ્કેરણી કરવા બદલ જાણીજોઈને ગંભીર તુકસાન પહોંચાડવું.
- ૧૨ ઈ.પી.કો. કલમ ૩૩૬ : અન્ય વ્યક્તિના જીવન અથવા સલામતીને જોખમમાં મૂકવું.
- ૧૩ ઈ.પી.કો. કલમ ૩૫૪ : જાતીય હેરાનગતિ/ત્રાસ આપવો.
- ૧૪ ઈ.પી.કો. કલમ ૩૫૪ : જાતીય સતામણી કરવી તથા તે  
(એ) બદલ સજા
- ૧૫ ઈ.પી.કો. કલમ ૩૫૪ : વોયરિઝમ (કોઈને જાતીય  
(સી) કુદ્રષ્ટીથી જોઈને આનંદ મેળવવો)
- ૧૬ ઈ.પી.કો. કલમ ૩૫૪ : ઓનલાઈન/ઓફલાઈન  
(ડી) સ્ટોકિંગ
- ૧૭ ઈ.પી.કો. કલમ : ચોરી  
૩૭૮/૩૭૯
- ૧૮ ઈ.પી.કો. કલમ : ખંડણી માંગવી.  
૩૮૩/૩૮૪
- ૧૯ ઈ.પી.કો. કલમ ૩૮૫ : ખંડણી મેળવવા માટે કોઈ વ્યક્તિને ઈજા કરવાના ભયમાં મૂકવા બાબત.
- ૨૦ ઈ.પી.કો. કલમ ૪૦૬ : ગુનાહિત વિશ્વાસઘાત કરવા માટેની સજા
- ૨૧ ઈ.પી.કો. કલમ ૪૧૯ : છળ દ્વારા છેતરપિંડી માટેની સજા
- ૨૨ ઈ.પી.કો. કલમ ૪૨૦ : છેતરપિંડી
- ૨૩ ઈ.પી.કો. કલમ ૪૬૫ : ખોટો દસ્તાવેજ બનાવવો.

- ૨૪ ઇ.પી.કો. કલમ ૪૬૮ : છેતરપિંડી માટે ખોટો દસ્તાવેજ બનાવવો.
- ૨૫ ઇ.પી.કો. કલમ ૪૬૯ : બદનામી માટે ખોટા ઇલેક્ટ્રોનિક દસ્તાવેજ બનાવવા.
- ૨૬ ઇ.પી.કો. કલમ ૪૭૧ : બનાવટી દસ્તાવેજનો અસલ તરીકે ઉપયોગ કરવો.
- ૨૭ ઇ.પી.કો. કલમ ૪૭૪ : ઇ.પી.કો. કલમ ૪૬૬ અને ૪૬૭માં વર્ણવેલા દસ્તાવેજ બનાવટી છે, તે જાણવા છતાં તેનો ઉપયોગ કરવો.
- ૨૮ ઇ.પી.કો. કલમ : બદનક્ષી  
૪૯૯/ ૫૦૦
- ૨૯ ઇ.પી.કો. કલમ ૫૦૩ : ગુનાહિત ઘાકઘમકી આપવી.
- ૩૦ ઇ.પી.કો. કલમ ૫૦૩ : ગુનાહિત ઘાકઘમકી માટેની સજા
- ૩૧ ઇ.પી.કો. કલમ ૫૦૭ : છૂપીરીતે કોમ્પ્યુનિકેશન સાધી ગુનાહિત ઘમકી આપવી.
- ૩૨ ઇ.પી.કો. કલમ ૫૦૮ : સ્ત્રીની મર્યાદાનું અપમાન કરવાના હેતુથી શબ્દો, હાવભાવ અથવા કૃત્ય કરવું.
- ૩૩ ઇ.પી.કો. કલમ ૫૧૧ : આજીવન કે અન્ય કેદની સજા સાથે સજાપાત્ર ગુનો કરવાનો પ્રયાસ કરવા બદલ સજા

લાગુ પડતી આઈ.ટી. એક્ટની કલમો

- ૧ આઈ.ટી. એક્ટ : કમ્પ્યૂટર સંબંધિત ગુનાઓ  
કલમ ૬૬
- ૨ આઈ.ટી. એક્ટ : ચોરી થયેલા કમ્પ્યૂટર  
કલમ ૬૬ (બી) સંસાધનો અથવા  
કોમ્યુનિકેશનને લગતાં  
ઉપકરણો અપ્રામાણિક રીતે  
ચોરી કરવા બદલ સજા
- ૩ આઈ.ટી. એક્ટ : કોઈ પણ અન્ય વ્યક્તિની  
કલમ ૬૬ (સી) ઓળખ આપવા બદલ સજા
- ૪ આઈ.ટી. એક્ટ : કોઈ પણ અન્ય વ્યક્તિની  
કલમ ૬૬ (ડી) ઓળખ આપી, કમ્પ્યૂટર વગેરે  
જેવાં ઉપકરણોની મદદથી  
છેતરપિંડી કરવા બદલ સજા
- ૫ આઈ.ટી. એક્ટ : ગુમતાના (પ્રાઈવસી) ભંગ  
કલમ ૬૬ (ઈ) બદલ શિક્ષા
- ૬ આઈ.ટી. એક્ટ : સાચબર ઉગ્રવાદ ફેલાવવા  
કલમ ૬૬ (એફ) બદલ સજા
- ૭ આઈ.ટી. એક્ટ : અશ્લીલ અથવા બીભત્સ  
કલમ ૬૭ બાબતો ઇલેક્ટ્રોનિક  
સ્વરૂપમાં પ્રસિદ્ધ કરવા  
અથવા મોકલવા માટે સજા

- ૮ આઈ.ટી. એક્ટ કલમ ૬૭ (એ) : જાતીય પ્રવૃત્તિઓ અથવા બાબતો વગેરે સ્પષ્ટપણે ઈલેક્ટ્રોનિક સ્વરૂપમાં પ્રસિદ્ધ કરવા અથવા મોકલવા માટે સજા
- ૯ આઈ.ટી. એક્ટ કલમ ૬૭ (બી) : બાળકોને જાતીય પ્રવૃત્તિઓ અથવા બાબતો કરતા સ્પષ્ટ રીતે ઈલેક્ટ્રોનિક સ્વરૂપમાં પ્રસિદ્ધ કરવા અથવા મોકલવા માટે સજા
- ૧૦ આઈ.ટી એક્ટ કલમ ૬૯ (એ) : ગેરકાનૂની જુગાર રમાડતી વેબસાઈટ્સ વગેરેને બ્લોક કરવા માટે
- ૧૧ આઈ.ટી. એક્ટ કલમ ૧૨૧ : ભારત સરકાર સામે લડત ચલાવવી અથવા યુદ્ધ કરવાનો પ્રયાસ કરવો, તેના માટે દુષ્પ્રેરિત કરવા.
- ૧૨ આઈ.ટી. એક્ટ કલમ ૧૨૧ (એ) : શિક્ષાપાત્ર ગુનાઓ કરવાનું કાવતરા બદલ સજા
- ૧૩ આઈ.ટી. એક્ટ કલમ ૧૨૨ : ભારત સરકાર સામે યુદ્ધ કરવાના હેતુથી હથિયારો વગેરે એકત્રિત કરવા.
- ૧૪ આઈ.ટી. એક્ટ કલમ ૧૨૪ (એ) : રાજદ્રોહ

લાગુ પડતા અન્ય અધિનિયમો અને તેને લગતી કલમો

- ૧ મહિલાઓને અયોગ્ય રીતે રજૂ કરવા અંગે, મહિલા અધિનિયમ (પ્રતિબંધ) ૧૯૮૬ ની કલમ ૪, ૬
- ૨ પ્રાઇઝ ચિટ્સ અને મની સર્ક્યુલેશન સ્કીમ્સ (પ્રતિબંધ) અધિનિયમ, ૧૯૭૮ ની કલમો ૩, ૪, ૫, ૬
- ૩ “મની લોન્ડરિંગ એક્ટ – ૨૦૦૨” અન્વયે લાગુ પડતી કલમો
- ૪ પબ્લિક ગેમ્બલિંગ એક્ટ ૧૮૬૭
- ૫ ફોરેન એક્ચેન્જ મેનેજમેન્ટ એક્ટ ૧૯૯૯ (FEMA)
- ૬ લોટરી રેગ્યુલેશન એક્ટ ૧૯૯૮
- ૭ રાજ્યએ બનાવેલ જુગાર વિરુદ્ધના કાયદા
- ૮ રિઝર્વ બેન્ક ઓફ ઈન્ડિયા અધિનિયમ ૧૯૩૪

રાજ્ય/દેશમાં કાયદાકીય રીતે નીચે મુજબના અપવાદ રહેલ છે.

- ૧ ભારત દેશમાં હોર્સ રેસિંગ કાયદાકીય રીતે ગેરકાનૂની કે ગુનાહિત પ્રવૃત્તિ માનવામાં આવતી નથી.
- ૨ અમુક રાજ્યમાં લોટરીનું આયોજન કરવું કે તેમાં ભાગ લેવો કાયદાકીય રીતે ગેરકાનૂની કે ગુનાહિત પ્રવૃત્તિ માનવામાં આવતી નથી.
- ૩ લોટરી રેગ્યુલેશન એક્ટ ૧૯૯૮, કૌશલ્યથી રમવામાં આવતી રમતને જુગારથી અલગ માને છે. કૌશલ્યથી રમવામાં આવતી રમતને કાયદાકીય રીતે ગેરકાનૂની કે ગુનાહિત પ્રવૃત્તિ માનવામાં આવતી નથી.

## ૧. મોબાઈલ રિચાર્જની દુકાન

મોબાઈલ રિચાર્જની દુકાન એક એવી જગ્યા છે, જ્યાં આરોપી તમારા મોબાઈલ નંબર અને તેનો કંટ્રોલ મેળવી શકે છે. કારણકે, તમે જ તેની પરવાનગી દુકાનદારને આપો છો. તેઓ તમને કોલ કરવા અથવા મેસેજ કરવા માટે તમારા નંબરનો દુરુપયોગ કરી શકે છે, તમારું શોષણ કરી શકે છે અથવા તમારી ભાવનાઓ સાથે દુર્વ્યવહાર અને માનસિક રીતે તમને ત્રાસ આપી શકે છે.

### લાગુ પડતી કલમો



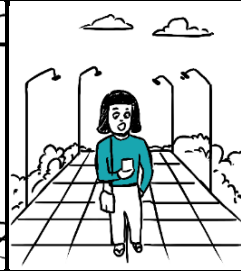

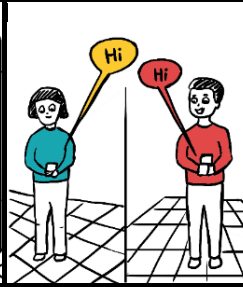

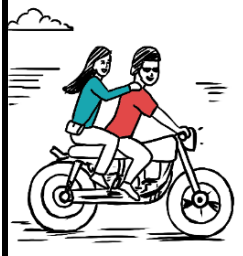


**દુકાનદારને લાગુ પડતી કલમો:–**

ઈ.પી.કો. કલમ ૩૫૪ (એ), ૩૫૪ (સી), ૩૮૩, ૩૮૪,  
૫૦૩, ૫૦૬, ૫૦૯

આઈ.ટી. એક્ટ કલમ ૬૬ (ઈ)

**દુકાનદાર દ્વારા મોબાઈલ નંબર વિષયક માહિતી અન્ય ગુનાહિત કૃત્ય સાથે સંકળાયેલ વ્યક્તિને વેચવામાં આવે છે ત્યારે દુકાનદાર પર લાગુ પડતી કલમો:–**

ઈ.પી.કો. કલમ ૧૦૯, ૧૧૪, ૧૨૦ (બી), ૪૦૬

		
<p>મીના રૂ. ૫૦નું રિચાર્જ કરવા માટે મોબાઇલ રિચાર્જની દુકાન પર ગયેલ</p>	<p>દુકાનદાર અબિલે તેને સર્વર ડાઉન હોવાના કારણે રિચાર્જ થવામાં સમય લાગશે તેમ જણાવેલ</p>	<p>અડધા કલાક પછી મીનાને તેના મોબાઇલમાં રૂ. ૫૦૦નું રિચાર્જ થયા હોવાનો મેસેજ આવ્યો.</p>
		
<p>તેણે અબિલને તેની પાસે રૂ. ૪૫૦ ન હોવાનું જણાવ્યું અબિલે પછીથી પૈસા આપવા કહ્યું.</p>	<p>અબિલ ત્યારબાદ તેને મેસેજ કરવા લાગ્યો અને થોડા જ સમયમાં બંને વચ્ચે મિત્રતા થઈ.</p>	<p>અબિલે, તે હંમેશાં મીનાની સાથે જ રહેશે તેમ વચન આપી તેને ગર્લફ્રેન્ડ બનવા પ્રપોઝ કર્યું.</p>
		
<p>મીના ખુશ થઈને અબિલ સાથે તેના બાઈક પર ફરવા લાગે છે. અબિલ તેને મોંઘી ગિફ્ટ ખરીદીને આપે છે.</p>	<p>અબિલ મીનાને સમજાવીને હોટેલમાં લઈ ગયો, જેના થોડા જ દિવસ પછી તેણે મીના સાથે બ્રેકઅપ કર્યું.</p>	<p>હવે અબિલ તેના વીડિયો વાઈરલ કરવાની ઘમઝકી આપી તેને ખૂબ બ્લેકમેઇલ કરે છે.</p>

## ૨. ડેબિટ કાર્ડ ક્લોનિંગ

ડેબિટ કાર્ડ સ્કિમિંગ એક પ્રકારનો ફ્રોડ છે, જેમાં છેતરપિંડી કરનાર વ્યક્તિ જો થોડી પળ માટે પણ તમારું કાર્ડ પોતાની પાસે મેળવી લે તો તેની નકલ કરી શકે છે. છેતરપિંડી કરનાર ત્યારપછી તમે નાણાંની ચુકવણી કરો અથવા અન્ય હેતુથી પિન નંબર દાખલ કરે ત્યારે તે તમારો પિન નંબર પણ જાણી લે છે. ત્યારબાદ તે કાર્ડ ક્લોનિંગ પદ્ધતિથી તેનું ડુપ્લિકેટ કાર્ડ બનાવી દે છે અને નાણાકીય ફ્રોડ કરે છે.

### લાગુ પડતી કલમો





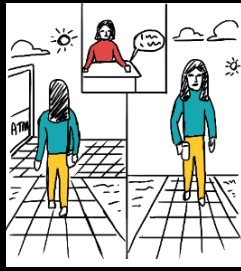

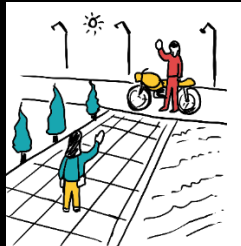

**ક્લોનિંગ માટે લાગુ પડતી કલમો:-**

આઈ.ટી. એક્ટ કલમ ૬૬, ૬૬ (સી), ૬૬ (ડી)

**ક્લોનિંગ થયા પછી પૈસાની લેવડદેવડ કરવા બદલ લાગુ પડતી કલમો:-**

ઈ.પી.કો. કલમ ૪૧૯, ૪૨૦



		
<p>મીના અને રીના બંને મિત્રો એક જ કોલેજમાં અભ્યાસ કરતાં હતાં.</p>	<p>મીનાનો બોયફ્રેન્ડ અર્જુન વ્યસની હતો, જે તેની પાસે હંમેશાં પૈસાની માંગણી કરતો.</p>	<p>અર્જુન ક્યારેક બદલાશે તેવી આશાએ મીનાએ તેને પૈસા આપવાનું ચાલુ રાખ્યું.</p>
		
<p>એક દિવસ મીના પાસે પૈસા ન હોઈ તેણે રીનાને પૈસા આપવા જણાવ્યું. રીનાએ પણ પૈસા ન હોઈ મીનાને ATM કાર્ડ અને પિનની માહિતી આપી.</p>	<p>મીનાએ ઝડપથી ATM થી રૂ. ૫૦૦ ઉઠાવ્યા અને રીનાને તેનું કાર્ડ પરત કર્યું.</p>	<p>એક અઠવાડિયા પછી રીનાને રૂ. ૫૦૦૦ નિકાળ્યા હોવાનો મેસેજ પ્રાપ્ત થયો. રીનાને ખૂબ જ આઘાત લાગ્યો.</p>
		
<p>જે દિવસે મીનાએ ATM કાર્ડ લીધું, અર્જુન બહાર રાહ જોઈ રહ્યો હતો. તેણે થોડા સમય માટે ATM કાર્ડ લઈ લીધું હતું.</p>	<p>એક સ્કિમિંગ ડિવાઈસથી તેણે તે કાર્ડની નકલ કરી હતી. તેની પાસે પિન હોવાથી ATMમાંથી પૈસા ઉપાડી લીધા.</p>	<p>ખૂબ જ સારો સંબંધ કે મિત્રતા હોય, તો પણ ક્યારેય કોઈને તમારું ATM કાર્ડ અને પિન આપશો નહીં.</p>

### ૩. કી લોગર

તે એક સ્પાયવેર છે, જે તમારા કમ્પ્યુટરમાં કી-બોર્ડ અને માઉસ વગેરે ઉપકરણોથી ટાઈપ કરવામાં આવતી માહિતી ગુનેગાર સુધી પહોંચાડે છે જેનાથી તે તમારા એકાઉન્ટની લોગઈન વિગત વગેરે માહિતી ચોરી કરી શકે છે.

#### લાગુ પડતી કલમો






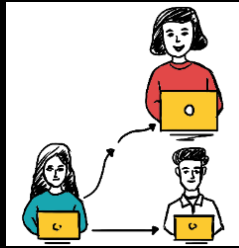


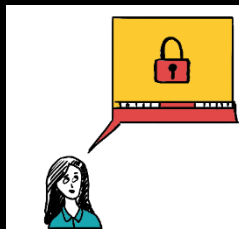
**કી લોગર ઈન્સ્ટોલ કરવા બદલ લાગુ પડતી કલમ:-**

આઈ.ટી. એક્ટ કલમ ૬૬

**અંગત માહિતી ચોરી કરી તેનો ઉપયોગ કરવા તથા નકલી પ્રોફાઈલ બનાવવી અને ખાનગી વાતચીત પોસ્ટ કરવા બદલ લાગુ પડતી કલમો:-**

આઈ.ટી. એક્ટ કલમ ૬૬ (સી), ૬૭, ૬૭ (એ)

ઈ.પી.કો. કલમ ૩૫૪ (એ), ૨૯૪

		
<p>અનુષા અને પૂજા સારા મિત્રો હતાં. તેઓ હોસ્ટેલમાં સાથે જ રહેતાં અને સાથે જ એક કંપનીમાં કામ કરતાં.</p>	<p>તેઓ બંને તેમના મેનેજર વિવેકને ખૂબ પસંદ કરતાં હતાં.</p>	<p>પૂજા વિવેક સાથે વધુ નિકટતા કેળવવા લાગે છે. હવે, તેઓ એકબીજાની સાથે વધુ સમય પસાર કરવા લાગ્યાં</p>
		
<p>અનુષાને આ બાબતનો આઘાત લાગ્યો હતો, હવે તે પૂજાને જિંદગીભર યાદ રહે તેવો પાઠ ભણાવવા માંગતી હતી.</p>	<p>અનુષા પૂજાની પ્રવૃત્તિઓ પર ધ્યાન રાખવા લાગી. તેણે પૂજાના લેપટોપમાં કી લોગર ઈન્સ્ટોલ કર્યું.</p>	<p>પૂજા અજાણા હતી કે, તેના પાસવર્ડ્સ, ફોટો અને અન્ય ખાનગી માહિતી ઉપર કોઈ નજર રાખી રહ્યું હતું.</p>
		
<p>અનુષાએ પૂજાની ખાનગી ચેટ અને અર્જુન સાથેના અંગત ફોટો સોશિયલ મીડિયા ઉપર નકલી પ્રોફાઇલ બનાવીને અપલોડ કર્યાં.</p>	<p>પૂજાએ તેના સાથેના સંબંધ જાહેર કર્યા તેવું સમજીને વિવેક પૂજા સાથે સંબંધ તોડે છે. બદનામીના ડરથી પૂજા પણ વ્યથિત થઈ ગઈ હતી.</p>	<p>પૂજાને અફસોસ થાય છે કે, તે પોતાને સુરક્ષિત રાખી શકે તે માટે તેણે કમ્પ્યુટરમાં એન્ટિ વાઈરસ ઈન્સ્ટોલ કરેલ ન હતો તેમજ પાસવર્ડ સેટ કરેલ ન હતો.</p>

## જ. મેસેજ સ્પૂફિંગ

સ્પૂફિંગ વડે પોતાનો નંબર છુપાવીને/ અન્ય અજાણ્યા નંબરથી અથવા કોઈ ચોક્કસ નંબર દર્શાવીને SMS મેળવનારને આ SMS ક્યાંથી અથવા કોના તરફથી આવેલ છે, તે જાણી ન શકાય તે રીતે SMS મોકલી શકાય છે. સામાન્ય રીતે SMS સ્પૂફિંગ વગર મોકલનાર વ્યક્તિ પોતાનો નંબર આ રીતે બદલી કે છુપાવી શકતી નથી. બદલવાથી અમુક લોકો આ રીતે SMS સ્પૂફિંગથી તમને અન્ય વ્યક્તિ કે કંપનીના નામે SMS મોકલીને છેતરી શકે છે.

### લાગુ પડતી કલમો

કોઈ ચુક્તિ અથવા છેતરપિંડીથી કોમ્યુનિકેશન કરી છેતરવાનું કાર્ય કરવા બદલ લાગુ પડતી કલમો:—

ઈ.પી.કો. કલમ ૪૧૯

આઈ.ટી. એક્ટ કલમ ૬૬ (સી), ૬૬ (ડી)

		
<p>એશ્વર્યા એક દુકાનદાર હતી. તે ઘણી ઈ-કોમર્સ સાઇટ્સ પર એક વિશેષ અધિકાર (Privileged) ધરાવતી હતી.</p>	<p>દરેક વખતે તે યોગ્ય ઓફર માટે રાહ જોઈને ઓછી કિંમતે ખરીદ કરતી હતી. તે કૂપન કોડ્સનો પણ ઉપયોગ કરતી.</p>	<p>એક દિવસ તેને ફિલપકાર્ટ તરફથી મેસેજ મળ્યો, જેમાં રૂ. ૫૦૦૦ની હેન્ડબેગ રૂ. ૫૦૦માં ઓફર કરવામાં આવેલ</p>
		
<p>તે જ મેસેજમાં લખેલ હતુ કે, જો ઓનલાઇન પેમેન્ટ કરવામાં આવશે તો તેને આ ઓફરનો લાભ બે વાર મળશે.</p>	<p>તેણે ઝડપથી બેંકમાં જઈ પોતાના ખાતામાં રૂ. ૧૦૦૦ જમા કર્યા અને આ ઓફરનો લાભ લેવા માટે ખરીદી કરી.</p>	<p>ઓર્ડર કર્યાને ઘણા દિવસો થઈ જવા છતાં ઓર્ડર મુજબ બેગ ન મળતા તેણે હેલ્પ-લાઇન નંબર પર કોલ કર્યો.</p>
		
<p>હેલ્પલાઇન નંબર પર વાત કરતા પોતે છેતરપિંડીનો ભોગ બની છે તેવો તેને અહેસાસ થયો.</p>	<p>તે મોટું કિસ્કાઉન્ટ મેળવવાની લાલચમાં ફિશિંગ અને મેસેજ સ્પૂફિંગનો ભોગ બની હતી.</p>	<p>ઈન્ટરનેટ પર ઘણા બધા લોકો નાઇજીરીયન કૌભાંડનો ભોગ બને છે. સાવચેત રહો સલામત રહો.</p>

## પ. કોલ સ્પૂફિંગ



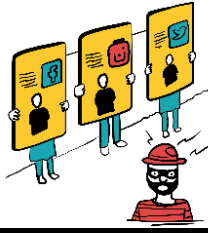


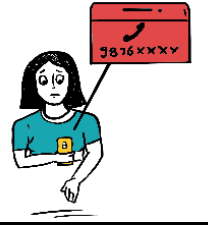



એપિલકેશન દ્વારા કોલ સ્પૂફિંગ થાય છે, જેમાં વ્યક્તિ ગુનાહિત ઈરાદો પાર પાડવા પોતાનો નંબર અને અવાજ બદલીને છેતરપિંડી કરે છે.

## લાગુ પડતી કલમો

કોઈ ચુક્તિ અથવા છેતરપિંડીથી કોમ્યુનિકેશન કરી છેતરવાનું કાર્ય કરવા બદલ લાગુ પડતી કલમો:—

ઈ.પી.કો. કલમ ૪૦૬, ૪૧૯

આઈ.ટી. એક્ટ કલમ ૬૬ (સી), ૬૬ (ડી)

		
<p>શબાના એક વિઘવા મહિલા હતી, તે એકલી રહેતી હતી.</p>	<p>પોતાને વ્યસ્ત રાખવા શબાના ઈન્ટરનેટનો ઉપયોગ કરતી અને સોશિયલ મીડિયા પર પણ ખૂબજ સક્રિય રહેતી.</p>	<p>તે સોશિયલ મીડીયા વિશે વધુ જાણતી ન હતી અને રિસ્કવેસ્ટ મોકલનાર તમામને તે મિત્ર બનાવતી હતી.</p>
		
<p>શબાનાના પુત્રએ એક વખત અચાનક તેને કોલ કરીને પોતાને ૧ લાખ રૂ.ની જરૂર હોવાનું જણાવ્યું, અને મિત્રના ખાતામાં પૈસા ટ્રાન્સફર કરવા માટે કહ્યું.</p>	<p>શબાનાને તેના જ ઈકરાના મોબાઈલ નંબર ઉપરથી ફોન આવતા તેણે બેનિફિશયરી એડ કરી ઝડપથી પૈસા ટ્રાન્સફર કર્યા.</p>	<p>પૈસા ટ્રાન્સફર કર્યા બાદ તેણે તેના ઈકરાને પૈસા પ્રાપ્ત થયા કે કેમ? તેમ પૂછવા માટે ફોન કર્યો.</p>
		
<p>તેનો ઈકરો, શફીક આશ્ચર્ય ચકિત થઈ, તેણે આ રીતે પૈસા આપવા માટે કોઈ કોલ કરેલ ન હોવાનું જણાવ્યું.</p>	<p>શબાનાને ખ્યાલ આવ્યો કે, પૈસા મેળવવા માટે કોલ સ્પૂફિંગ થઈ તેના ઈકરાના નંબરનો ઉપયોગ કરી ખોટી વ્યકિતએ તેને ફોન કર્યો હતો.</p>	<p>ચોક્કસ એપ્લિકેશન્સથી કોઈ પણ ફોન નંબરથી કોલ અને SMS કરી શકાય છે. આ ટેકનિકનો ઉપયોગ ખરાબ લોકો અન્યને છેતરવા માટે કરે છે. સાવચેત રહો.</p>

## ૬. રેન્સમવેર

રેન્સમવેર એક માલવેર છે, જે તમારી ફાઇલોને એન્ક્રિપ્ટ કરે છે, જેથી આપ આપની ફાઇલ્સ/ ડેટાનો ઉપયોગ કરી શકતા નથી. હુમલાખોર આપની જ ફાઇલ્સ ડિક્રિપ્ટ કરવા માટે આપની પાસે ખંડણી માંગે છે, જેથી આપ આપની ફાઇલ્સ/ ડેટા અગાઉની જેમ પુનઃ ઉપયોગ કરી શકો. અહીં ખંડણી સામાન્ય રીતે સો રૂપિયાથી લઈને હજારો રૂપિયા સુધીની હોઈ શકે છે, જે બિટકોઈનમાં ચૂકવવા જણાવવામાં આવે છે.

### લાગુ પડતી કલમો

અનધિકૃત પ્રવેશ તથા પોતાની જ માલિકીની વસ્તુ ઉપયોગમાં ન લેવા દેવા બદલ હુમલાખોર પર લાગુ પડતી કલમ:-

આઈ.ટી. એક્ટ કલમ ૬૬

નાણાંની માંગણી કરવા બદલ લાગુ પડતી કલમ:-

ઈ.પી.કો. કલમ ૩૮૪



<p>એલીશા સ્વતંત્ર બિઝનેસ કરતી હતી. તેની કંપનીમાં ૫૦ કર્મચારીઓ અને ૬૦ કમ્પ્યુટર સિસ્ટમ્સ હતી.</p>	<p>એક દિવસ એલીશાને તેના ગ્રાહક પાસેથી એક ઈ-મેઇલ મળ્યો. એલીશાએ ઈ-મેઇલમાં આવેલ ફાઇલ ઓપન કરી.</p>	<p>તેના કમ્પ્યુટરમાં એન્ટિ વાઇરસ અપડેટ ન હોઈ તેને ફાઇલ ખોલવા બાબતે કોઈ ચેતવણી મળી નહીં.</p>
<p>ફાઇલ ખોલતાની સાથે જ, તેનું કમ્પ્યુટર લોક થઈ ગયેલ અને બધી ફાઇલો પણ એન્ક્રિપ્ટ થઈ ગયેલ. તે કમ્પ્યુટર વાપરી શકતી નથી.</p>	<p>કમ્પ્યુટર પર એક મેસેજ આવવા લાગે છે કે, જો કમ્પ્યુટર અનલોક કરવું હોય તો એક લાખ રૂ. બિટકોઇનમાં ચૂકવવાના રહેશે.</p>	<p>તેના કમ્પ્યુટરમાં અગત્યની માહિતી હોઈ એલીશાએ જણાવેલ બિટકોઇન વોલેટના સરનામા પર ચૂકવણી કરી દીધી.</p>
<p>પૈસા ચૂકવ્યા છતાં પણ તેને કમ્પ્યુટર અનલોક કરવા માટેની જરૂરી 'કી' મળતી નથી. તેની ફાઇલ્સ એન્ક્રિપ્ટેડ જ રહે છે.</p>	<p>તેના મેનેજરે જણાવ્યું કે, તેને જે ઈ-મેઇલ પ્રાપ્ત થયેલ તે રેન્સમવેર વાઇરસ સાથેનો ફિશિંગ ઈ-મેઇલ હતો.</p>	<p>એલીશાને તે ઈ-મેઇલ ડીલીટ ન કરવા તથા એન્ટિ વાઇરસ અપડેટ ન રાખવા બદલ અફસોસ થાય છે. એન્ટિ વાઇરસ હંમેશાં અપડેટ કરો.</p>



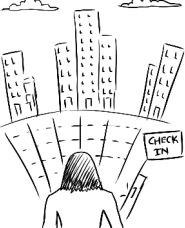
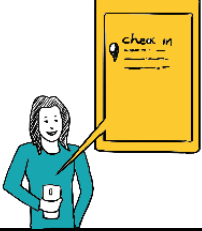




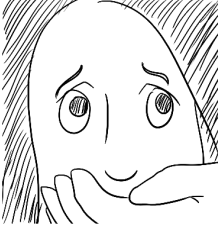
### ૭. સાચબર સ્ટોકિંગ

ઇન્ટરનેટ અથવા અન્ય ઇલેક્ટ્રોનિક્સ માધ્યમ/ ઉપકરણથી કોઈને સતત હેરાન કરવું, તેઓના વિશે સોશિયલ મીડિયા ઉપર અપલોડ કરેલ માહિતીનો દુરુપયોગ કરી તેમને હેરાન – પરેશાન કરવું વગેરેને સાચબર સ્ટોકિંગ કહે છે.

### લાગુ પડતી કલમો

**ઓનલાઇન/ ઓફલાઇન:–**

ઇ.પી.કો. કલમ ૩૫૪, ૩૫૪ (ડી)

		
<p>સીમા એક NRI હતી, તે અમેરિકાથી ભાઇતર પૂર્ણ કરીને ઉચ્ચ અભ્યાસ કરવા માટે ભારતમાં આવી હતી. તે નિખાલસ સ્વભાવની હતી.</p>	<p>તે જે પણ કરતી હતી, તેને સોશિયલ મીડિયા પર અપલોડ કરતી, તેના ૧૦,૦૦૦ કરતાં વધુ ફોલોઅર્સ હતા.</p>	<p>તે ચેક-ઇન સુવિધાનો ઉપયોગ કરતી, પોતે ક્યાં ફરે છે તેના વિશે અપડેટ કરતી. પોતાની અંગત ઘણી માહિતી તે ઓનલાઇન શેર કરતી.</p>
		
<p>એક દિવસ તેણે સોલો ટ્રીપ પર ગોવા જવાનું નક્કી કર્યું. તેણે પોતાના સોશિયલ મીડિયામાં પોતાના પ્રવાસ વિશેની માહિતી મૂકી હતી.</p>	<p>કિરણ નામનો એક અજાણ્યો યુવક તેની તમામ વિગતો પર નજર રાખતો હતો. તે ગુનેગાર હતો અને હાલ જામીન પર બંદાર આવ્યો હતો.</p>	<p>કિરણે તુરંત ગોવા જવા માટે બસ પકડી અને સીમાની જ હોટેલમાં રૂમ રોકાયો. તેણે સીમાને મેસેજ કર્યો અને મળવાની ઇચ્છા વ્યક્ત કરી.</p>
		
<p>સીમાએ તેની પ્રોફાઇલને ચકાસીને તેને બ્લોક કરી દીધો, પરંતુ કિરણના ઇરાદા વિશે તે અજાણ હતી.</p>	<p>કિરણ સીમાનો પીછો કરતાં કરતાં બીચ પર તેની પાછળ પાછળ ગયો અને જ્યારે તેની આસપાસ કોઈ ન હતું ત્યારે તેની છેડતી કરી ભાગી ગયો.</p>	<p>સીમા ડરી ગઈ, તેને સોશિયલ મીડિયા પર અપલોડ, અપડેટ્સ અને પોરટ્સ કરવા બદલ પોતાની ભૂલ સમજાઈ. તમે પણ કાળજી રાખજો.</p>

## ૮. ફોટો મોફિંગ

સોશિયલ નેટવર્કિંગ સાઈટ્સ પર અથવા અન્ય રીતે કોઈના દ્વારા મૂકવામાં આવેલ ફોટાનો ઉપયોગ કરીને તેઓના ચહેરા અને અન્યના શરીરનો ઉપયોગ કરીને તસવીર બનાવવી અને આ રીતે તૈયાર કરેલ તસવીરનું બ્લેકમેઈલ કરવા અથવા અન્યથા વ્યક્તિને ડરાવવા માટે પ્રકાશિત કરવું કે ઉપયોગ કરવો અને તે રીતે ફોટો મોફિંગ કરીને વ્યક્તિનું શોષણ કરવું.

### લાગુ પડતી કલમો

ઈ.પી.કો. કલમ ૨૯૨, ૪૬૫, ૪૬૯, ૫૦૭, ૫૦૯

આઈ.ટી. એક્ટ કલમ ૬૬(સી), ૬૭, ૬૭ (એ)

મહિલાઓને અયોગ્ય રીતે રજૂ કરવા અંગે, મહિલા અધિનિયમ(પ્રતિબંધ) ૧૯૮૬ ની કલમ ૪, ૬



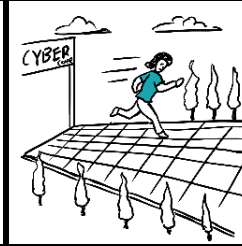






<p>એશ્વર્યા એક ૧૮ વર્ષની ખુશમિજાજી અને ભોળી કિશોરી હતી, તે મુંબઈમાં રહેતી હતી.</p>	<p>તે હંમેશાં તેના નવા ફોટો પાડીને ઈન્ટર પર અપલોડ કરતી હતી. તેને ટીકટોક પણ ગમતું હતું.</p>	<p>તેના દરેક ફોટો પર હજારો લાઈક્સ અને કોમેન્ટ્સ આવતી હતી.</p>
<p>એક દિવસ એશ્વર્યાને એક અજાણી વ્યક્તિની ફ્રેન્ડ રિકવેસ્ટ આવી, જે તેણે સ્વીકારી હતી.</p>	<p>આર્યન નામનો યુવક તેને સોશિયલ મીડિયા પર ફોલો કરતો હતો, આર્યને એશ્વર્યાની કોલેજ જઈને તેને પ્રપોઝ કર્યું.</p>	<p>એશ્વર્યાએ તેનો અસ્વીકાર કર્યો. તેણે આર્યન પર ગુસ્સો કરીને તેને અપમાનિત કર્યો.</p>
<p>આર્યન પોતાના ઘરે જઈ એશ્વર્યાના ફોટો ડાઉનલોડ કરી તેને બીબલ્સ ફોટો સાથે મોર્ફ કરવા લાગ્યો.</p>	<p>તેણે મોર્ફ કરેલા ફોટો તેના મિત્રોને મોકલ્યા અને તેના ફોનનંબર સાથે વિવિધ વેબસાઈટ્સ પર પણ અપલોડ કર્યા.</p>	<p>એશ્વર્યા હતાશાનો શિકાર બની ગઈ હતી. તમારા અંગત ફોટો અપલોડ કરશો નહીં. અજાણી વ્યક્તિની ફ્રેન્ડ રિકવેસ્ટ સ્વીકારશો નહીં.</p>

### ઢ. પ્રોફાઈલ હેકિંગ

મોટા ભાગે સાચબર સ્ટોકિંગ કરનાર વ્યકિત ઢ્ઘારા તમારા ઁકાઉઝ્ટ અથવા સોશિયલ નેટવર્કિંગ પ્રોફાઈલમાં લોગઈન કરવાની વિગત મેળવી લેવામાં આવે છે અને પછીથી તેનો અચોગ્ય રીતે ઉપયોગ કરવામાં આવે છે.

### લાગુ પડતી કલમો

આઈ.ટી. ઁક્ટ કલમ ૬૬, ૬૬ (સી)

		
<p>તનુજા ઈન્ટરનેટ સર્ફિંગ કરવા માટે સાયબર કાફેમાં જવાનું પસંદ કરતી હતી.</p>	<p>કાફેમાં તે તેનું ફેસબુક અને જીમેઇલ ખુલ્લું રાખતી, એક દિવસ ફેસબુક પર તે તેના મિત્રો સાથે વાત કરતી હતી.</p>	<p>તેના ઘરેથી ફોન આવ્યો કે, તેના દાદા અચાનક બેભાન થઈ ગયા હોઈ તેમને હોસ્પિટલમાં દાખલ કરવામાં આવ્યા છે.</p>
		
<p>તે તેના દાદાને ખૂબ પ્રેમ કરતી હોવાથી તુરંત હોસ્પિટલમાં જવા માટે ચાલી ગઈ.</p>	<p>હોસ્પિટલ પહોંચ્યા પછી તનુજાને ફોન પર બે સંદેશા પ્રાપ્ત થયા કે, જેમાં જીમેઇલ તથા ફેસબુકના પાસવર્ડ રિસેટ કરવામાં આવેલ હતા.</p>	<p>તનુજાને સમજાયું કે, તેણે ફેસબુક અને જીમેઇલમાંથી લોગ આઉટ કર્યું ન હતું, જેથી તેના એકાઉન્ટમાં ચેડાં થયેલ હતાં.</p>
		
<p>સાર્વજનિક કમ્પ્યુટરનો ઉપયોગ કરતી વખતે લોગ આઉટ કરવાનું હંમેશાં યાદ રાખો.</p>	<p>પાસવર્ડ અને અન્ય સંવેદનશીલ માહિતી દાખલ કરતી વખતે વર્ચ્યુઅલ કીબોર્ડનો ઉપયોગ કરો.</p>	<p>રેસ્ટોરન્ટ્સ/એરપોર્ટ જેવી જાહેર જગ્યાઓ પર ફ્રી WIFIનો ઉપયોગ કરવાનું ટાળો, જરૂર હોય તેવા સમયે VPN નો ઉપયોગ કરો.</p>

## ૧૦. ઓનલાઈન ગેમ્સ

જે વ્યક્તિમાં એકલતા, આત્મવિશ્વાસનો અભાવ અને વઘારે પડતી સંવેદનશીલતા હોય છે તેઓને ખતરનાક ઓનલાઈન ગેમ્સની આદત લાગી જાય છે અને તેનો શિકાર બને છે. બ્લૂ વ્હેલ ચેલેન્જ જેવી કેટલીક ખતરનાક ઓનલાઈન ગેમ્સ પીડિતના જીવનનો અંત લાવે છે. આવી ગેમ્સ એક સામાજિક પડકાર છે.

### લાગુ પડતી કલમો

ઈ.પી.કો. કલમ ૩૦૫, ૩૦૬, ૩૩૭



<p>દેવિકા એન્જિનિયરિંગમાં અભ્યાસ કરતી કિશોરી હતી. તેનાં માતાપિતા નાનકડા ગામડામાં રહેતાં હતાં.</p>	<p>તે ખૂબજ સાદગીથી રહેતી હોઈ કોલેજમાં કોઈ તેની સાથે વાત કરતા ન હતા. સોશિયલ મીડીયામાં પણ તેનું કોઈ મિત્ર ન હતું.</p>	<p>એક દિવસ તેને ઇ-મેઇલથી બ્લૂટૂલ ગેમ પ્રાપ્ત થઈ, ઇન્ટરોલ કરતા જ સ્કીન ઉપર “તમે તૈયાર છો?” તેવો મેસેજ આવ્યો.</p>
<p>દેવિકા આ રમત રમવા માટે ઉત્સાહિત હતી. ગેમમાં ૫૦ સ્ટેજ હતા. દરેક સ્ટેજમાં એક ચેલેન્જ પૂર્ણ કરવાની હતી.</p>	<p>ચેલેન્જ પૂર્ણ કરવાથી તેને પોઈન્ટ મળતા હતા. તેને ગેમ ખૂબ ગમવા લાગી હતી અને સતત ગેમ રમવાના કારણે તેને ગેમની આદત પડી ગઈ.</p>	<p>ખતરનાક ચેલેન્જ જેવી કે, રાત્રીથી લઈને સવાર સુધી શરીર પર છરી દ્વારા નિશાન કરવાના, વગેરે ચેલેન્જ તે ગેમમાં સોંપવામાં આવતી.</p>
<p>તેનામાં આવેલ પરિવર્તનની તેની આસપાસના લોકોએ પણ નોંધ ન લીધી.</p>	<p>અંતિમ ટાસ્ક ફાંસી લગાવી આત્મહત્યા કરવાનું હતું. તેણે ફાંસી પહેલા તેનાં માતાપિતાને એક માફીપત્ર લખ્યો.</p>	<p>તેણે લખ્યું હતું, “હું ઇચ્છતી હતી કે, લોકો મને પ્રેમ કરે, મને અવગણવામાં આવી જેથી મારે નથી જીવવું.</p>

## ૧૧. જોબ ફોડ

નોકરીઓ આપતી વેબસાઈટ્સની સત્યતા અને યોગ્યતા ચકાસવાની જરૂર છે. આ બાબતે તમારા ઈ-મેઈલ એકાઉન્ટન્ટમાં જ્યારે ઈ-મેઈલ આવે છે અને તમે તેના પર જવાબ આપો છો. અને તેના પર કાર્ય કરો છો તે પહેલાં ઈ-મેઈલને બેવાર તપાસવા અને તેની ચકાસણી કરવી જરૂરી છે, ખાસ કરીને જ્યારે આપને વ્યક્તિગત માહિતી મોકલવાનું કહેવામાં આવે.

### લાગુ પડતી કલમો

ફેક એકાઉન્ટ અને આઈ.ડી. નો ઉપયોગ કરવા બદલ લાગુ પડતી કલમો:-

આઈ.ટી. એક્ટ કલમ ૬૬ (સી), ૬૬ (ડી)

ઈ.પી.કો. કલમ ૪૦૬, ૪૧૯, ૪૨૦, ૪૬૫, ૪૬૮, ૪૭૧,  
૪૭૪, ૧૨૦ (બી)

		
<p>નિશીતાએ પ્રથમ વર્ગ સાથે તેનો ઉચ્ચ અભ્યાસ કરેલ હતો. પરંતુ, કોલેજ પ્લેસમેન્ટથી તેને નોકરી મળી ન હતી.</p>	<p>સારી નોકરી મેળવવાની આશાએ તેણે naukari.com, અને અન્ય વેબસાઈટ્સ પર તેની વિગત અપલોડ કરી હતી.</p>	<p>એક દિવસ તેને પ્રતિષ્ઠિત કંપની તરફથી નોકરી માટે ઈ-મેઈલથી ઓફર આવી, સેલેરી પણ આકર્ષક હતી.</p>
		
<p>નિશીતાનું ઈન્ટરવ્યૂ એક ફાઈવ સ્ટાર હોટેલમાં સુનિશ્ચિત કરવામાં આવ્યું, તે રિક્ષા દ્વારા હોટેલે પહોંચી.</p>	<p>તેને સ્યુટરૂમ તરફ જવા જણાવવામાં આવ્યું, જ્યાં અન્ય લોકો પણ નોકરી માટે આવ્યા હતા.</p>	<p>નિશીતાનું ઈન્ટરવ્યૂ શરૂ થયું. શરૂઆતમાં જ તેને એક પીણું આપવામાં આવ્યું. તે પીતા જ તે બેભાન થઈ ગઈ.</p>
		
<p>નિશીતાને પીણું પીધા પછી તેની સાથે શું થયું તે યાદ ન હતું, તે નિર્વસ્ત્ર અવસ્થામાં પથારી પર હતી, તેનું ચૌન શોષણ થયું હતું.</p>	<p>નિશીતાને અહેસાસ થયો કે, તે ફિશિંગ ઈ-મેઈલનો ભોગ બની છે. તેને ઈ-મેઈલ કે જોબ ઓફરની ખરાઈ કરી ન હતી.</p>	<p>નિશીતાની જેમ ઘણી મહિલાઓનું નોકરીના બહાને શારીરિક અને આર્થિક શોષણ થાય છે. તમે આ બાબતે કાળજી રાખો.</p>

## ૧૨. ડીપ ફેક

ડીપ ફેક એ એક તકનીક છે, જેના ઉપયોગથી નવી ઇમેજ અને વીડિયોને તમારા ઇમેજ અને વીડિયો સાથે એ રીતે જોડવામાં આવે છે કે, જેમાં અવાજ અને ચહેરાને જોનાર તથા સાંભળનારને એવું લાગે કે, આ ઇમેજ કે વીડિયો ઓરિજિનલ છે.

### લાગુ પડતી કલમો

**ફેક એકાઉન્ટ અને આઈ.ડી. નો ઉપયોગ કરવા બદલ લાગુ પડતી કલમ:-**




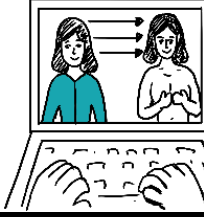
આઈ.ટી. એક્ટ કલમ ૬૬ (સી)

**ઓનલાઈન પ્રસિદ્ધ કરવા બદલ લાગુ પડતી કલમો:-**

આઈ.ટી. એક્ટ કલમ ૬૭, ૬૭ (એ)

**સ્ટોકિંગ:-**

ઈ.પી.કો. કલમ ૩૫૪ (એ), ૩૫૪ (ડી), ૪૬૫

		
<p>જેનેટ MBBSના અંતિમ વર્ષમાં અભ્યાસ કરતી યુવતી હતી. તે અને જહોન ૩ વર્ષથી એકબીજાને પસંદ કરતાં હતાં.</p>	<p>તે નિયમિત રીતે રોજ ટીકટોક અને ઈન્સ્ટાગ્રામ પર ઓછામાં ઓછી બે પોસ્ટ્સ અપલોડ કરતી હતી.</p>	<p>એકવાર જેનેટ અને જહોન વચ્ચે ઝઘડો થતાં બંને વચ્ચે બ્રેકઅપ થયું, કોલેજમાં અન્ય યુવક અર્જુનને તેની ખબર પડી.</p>
		
<p>અર્જુનને તેનો લાભ ઉઠાવી જેનેટને પ્રપોઝ કર્યું અને તે સંમત થઈ ગઈ. પરંતુ જહોનનો તિરસ્કાર કરવા બદલ તેને પછીથી અફસોસ થયો.</p>	<p>એક સપ્તાહની અંદર અર્જુન સાથે બ્રેકઅપ થતા તેણે જહોનની પાસે માફી માંગતા જહોને તેને માફ કરેલ.</p>	<p>જેનેટ સાથે બ્રેકઅપ થતા વિચલિત થયેલ અર્જુન બદલાની ભાવનાથી તેને પાઠ શીખવવા માંગતો હતો.</p>
		
<p>અર્જુન ઈન્સ્ટાગ્રામ અને ટીકટોકના ફોટો અને વીડિયોમાં ટૂલનો ઉપયોગ કરી ડીપફેક બનાવવા લાગ્યો.</p>	<p>આ ડીપફેક વીડિયોમાં જેનેટને એક કરતાં વધુ લોકો સાથે વ્યાભિચાર કરતી બતાવવામાં આવી હતી. તેણે આ વીડિયો સોશિયલ મીડિયામાં અપલોડ કર્યાં.</p>	<p>મોટાભાગના લોકોએ આ વીડિયો પર વિશ્વાસ કર્યો. જેનેટ પોતાના ફોટો અને વીડિયો સોશિયલ મીડિયામાં અપલોડ થતાં ખૂબ દુઃખી થઈ હતી.</p>

### ૧૩. ડેટિંગ વેબસાઈટ

સ્ત્રીની સાથે લોભામણી વાતો કરનાર ડેટિંગ વેબસાઈટ પર તેઓને પ્રેમમાં ફસાવી શકે છે અને તેઓની ભાવનાને આહત કરી શકે છે. કોઈ પણ ખાનગી ફોટો કે મેસેજ મેળવી ડેટિંગ વેબસાઈટ્સના માધ્યમથી આપનો સંપર્ક કરનાર વ્યક્તિ આપને બ્લેકમેઇલ કરી શકે છે.

### લાગુ પડતી કલમો

આઈ.ટી. એક્ટ કલમ ૬૬ (સી), ૬૬ (ડી)

ઈ.પી.કો. કલમ ૪૧૯, ૪૨૦

**ઓનલાઈન પ્રસિદ્ધ કરવા બદલ લાગુ પડતી કલમો:—**

આઈ.ટી. એક્ટ કલમ ૬૭, ૬૭ (એ)

ઈ.પી.કો. કલમ ૪૬૫, ૫૦૭, ૫૦૯

		
<p>રશિમ MBBSના પ્રથમ વર્ષમાં અભ્યાસ કરતી હતી. તે મિસ ફેશર પ્રતિયોગિતામાં વિજેતા થઈ હતી.</p>	<p>તે હંમેશાં ઓનલાઇન મિત્રો સાથે વાત કરતી, પરંતુ હવે તે એકની એક જ વ્યક્તિઓ સાથે વાતો કરી કંટાળી હતી.</p>	<p>એક દિવસ તે ટિન્ડર પર એકાઉન્ટ બનાવીને નવા મિત્રોની શોધ કરવા લાગી.</p>
		
<p>એક દિવસ એપ થકી તેની મુલાકાત એક સુંદર ટેખાતા યુવક સાથે થઈ, તેની પાસે મોંઘી કાર હતી, તે હરવા-ફરવાનો શોખીન હતો.</p>	<p>તે ખૂબ સારી રીતે વાતો કરતો હતો. રશિમ તેનાથી ખૂબ પ્રભાવિત થઈ અને પોતાને ખૂબ ભાગ્યશાળી સમજવા લાગી.</p>	<p>તે વ્યક્તિ તેને કેન્ડલ લાઇટ ડિનર માટે લઈ ગયો, રશિમ તેને મનોમન ચાહવા લાગી.</p>
		
<p>એક દિવસ તેણે રશિમને જણાવ્યું કે, આઈ.ટી. વિભાગ તરફથી તેના એકાઉન્ટ બ્લોક કરી દેવામાં આવેલ છે. તેને બે લાખ રૂ. ની ખૂબ જરૂર છે. રશિમએ તેને પૈસા આપ્યા.</p>	<p>થોડા દિવસો પછી તે વ્યક્તિ રશિમને બ્લોક કરી દે છે, પછીથી રશિમને જાણ થાય છે કે, તે વ્યક્તિ પરિણીત હતી અને આ રીતે તે યુવતીઓ પાસેથી પૈસા પડાવી તેમને તરછોડી મૂકતો હતો.</p>	<p>હવે તેને પરતાવો થાય છે કે, તેને હેટિંગ સાઈટના માધ્યમથી મળેલ અજાણી વ્યક્તિનો ભરોસો કર્યો. સાવચેત રહો, સલામત રહો.</p>

## ૧૪. કેમેરા હેકિંગ

આપના ફોનમાં અટેચમેન્ટ સાથે માલવેર ડાઉનલોડ કરવામાં આવે છે અથવા અન્ય રીતે દાખલ કરવામાં આવે છે. તેના દ્વારા આપના ફોટોગ્રાફ આપની સંમતિ વિના લેવામાં આવે છે, આ રીતે કેમેરા હેકિંગ થાય છે.

### લાગુ પડતી કલમો

#### હેકિંગ:-

આઈ.ટી. એક્ટ કલમ ૬૬

#### ફોટોગ્રાફ્સ લેવા વીડિયોગ્રાફી કરવી:-

ઈ.પી.કો. કલમ ૩૫૪ (એ), ૩૫૪ (સી), ૪૧૯

આઈ.ટી. એક્ટ કલમ ૬૬ (ઈ)

#### સ્ટોકિંગ:-

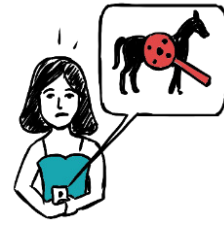

ઈ.પી.કો. કલમ ૩૫૪D

#### ઓનલાઈન પ્રસિદ્ધ કરવા બદલ લાગુ પડતી કલમો:-

આઈ.ટી. એક્ટ કલમ ૬૭, ૬૭ (એ)

ઈ.પી.કો. કલમ ૫૦૭, ૫૦૯



		
<p>મનીષા ફેશન ડિઝાઇનર હતી. તે ખૂબ જ હોશિયાર હતી. તે સ્માર્ટફોનનો ખૂબ ઉપયોગ કરતી હતી.</p>	<p>ફોનથી જ તે ઈ-મેઇલ ચેક કરતી, સોશિયલ મીડિયા એકાઉન્ટ્સ મેનેજ કરતી અને બેન્ક એકાઉન્ટ પણ વાપરતી.</p>	<p>તેને હંમેશાં તેનો ફોન વોશરૂમ સહિત તમામ જગ્યાએ સાથે લઈ જવાની ટેવ હતી.</p>
		
<p>તેને ખ્યાલ ન હતો કે, તેણે મેસેન્જર પરથી ડાઉનલોડ કરેલી ફાઇલ એક માલવેર વાઈરસ ફાઇલ હતી.</p>	<p>માલવેર તેની સંમતિ વિના તેના ફોનના કેમેરાથી તેનો વીડિયો કેપ્ચર કરતો હતો.</p>	<p>માલવેર વિશે તે અજાણ હતી, મનીષાએ પોતાનો ફોન બાથરૂમમાં એક બાજુ રાખ્યો અને નાહવા લાગી.</p>
		
<p>એક દિવસ, તેના મિત્રએ તેને કહ્યું કે, એક અયોગ્ય વેબસાઈટ પર તેનો નાહતો વીડિયો અપલોડ થયો છે.</p>	<p>મનીષાને અહેસાસ થયો કે, તેના ફોનમાં એન્ટી વાઈરસ ઈન્સ્ટોલ નથી કે, જે ફોનનું રક્ષણ કરે.</p>	<p>તેને ફોનના કેમેરા ઢાંકીને ન રાખવા તથા તમામ જગ્યાએ ફોન સાથે રાખવા બદલ અફસોસ થયો. તમે પણ કાળજી રાખો.</p>

## ૧૫. સોશિયલ ટ્રોલિંગ

સોશિયલ ટ્રોલિંગ એટલે કોઈ વ્યક્તિ અથવા સંસ્થા, સંગઠન વિશે ભડકાઉ લખાણ અથવા ફોટો સોશિયલ મીડિયામાં પોસ્ટ કરી જે તે વ્યક્તિ, સંસ્થા, સંગઠન વિશે અપમાન અથવા પરેશાન કરવાના હેતુથી કરવામાં આવતું કૃત્ય.

### લાગુ પડતી કલમો

ઈ.પી.કો. કલમ ૫૦૦, ૫૦૩, ૫૦૭, ૫૦૯

સ્ટોકિંગ:-

ઈ.પી.કો. કલમ ૩૫૪ (ડી)

<p>શ્રુતિ એક મધ્યમ વર્ગ પરિવારમાં રહેતી હતી. તે સ્વભાવે સરળ હતી. તેને નૈતિકતામાં વિશ્વાસ હતો.</p>	<p>તે જે કોલેજમાં અભ્યાસ કરતી હતી, ત્યાંના વિદ્યાર્થીઓ ખૂબ નેદરકાર અને ફેશનેબલ હતા.</p>	<p>તેઓ શ્રુતિની ખૂબ મજાક-મશ્કરી કરતા અને તેને માનસિક ત્રાસ આપતા હતા.</p>
<p>કોલેજમાં સૌથી પ્રખ્યાત છોકરો રોહન શ્રુતિને અભાલ અને ગાંડી કહીને બોલાવતો અને તે શ્રુતિને તેના ગામમાં પાછા જવા માટે કહેતો હતો.</p>	<p>શ્રુતિએ આ લોકોથી દૂર રહેવાનું નક્કી કર્યું. એકવાર તેણે હિંમત કરીને રોહનને ખૂબ ધમકાવ્યો હતો અને પોતાને પરેશાન ન કરવા કહી દીધું.</p>	<p>ગુસ્સે થઈને રોહન પાછો ઘરે જઈને શ્રુતિના નામ સાથે ખરાબ જોક્સ જોડીને તેના મિત્રોને મોકલવા લાગ્યો.</p>
<p>રોહન ટ્રોલ પેજ બનાવીને તેમાં શ્રુતિના ફોટો અને રમૂજ વીડિયો અપલોડ કરવા લાગ્યો.</p>	<p>જેથી શ્રુતિ કોલેજમાં તમામ માટે હાસ્યને પાત્ર બની હતી. હવે, તેણે અભ્યાસ છોડવાનું નક્કી કર્યું હતું.</p>	<p>શ્રુતિને અહેસાસ થયો કે, તેણે કોલેજના સત્તાધિકારીઓને જાણ કરવી જોઈએ અને મહિલા પોલીસ સ્ટેશનમાં ફરિયાદ કરવી જોઈએ.</p>

## ૧૬. પોન્ઝી સ્કીમ





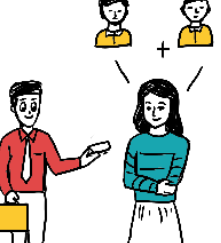
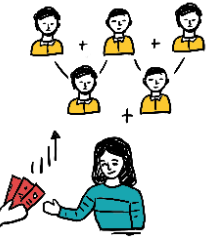



કોઈ વ્યક્તિ અથવા સમૂહ દ્વારા અન્ય વ્યક્તિઓને ખૂબ જ આકર્ષક જણાઈ આવતી અવાસ્તવિક એવી લોભામણી જાહેરાત કરીને રોકાણ કરવા માટે જણાવવામાં આવે છે, જેમાં રોકાણકર્તાને ખૂબ જ ઊંચા વ્યાજદર આપવાનું વચન આપવામાં આવે છે. અને ત્યારબાદ આ પ્રકારની લાલચ આપનાર સમૂહ એકઠા કરવામાં આવેલ રોકાણકર્તાનાં નાણાં લઈને નાસી જાય છે.

### લાગુ પડતી કલમો

પ્રાઈઝ ચિટ્સ અને મની સર્ક્યુલેશન સ્કીમ્સ (પ્રતિબંધ) અધિનિયમ, ૧૯૭૮ ની કલમો ૩, ૪, ૫, ૬

ઈ.પી.કો. કલમ ૩૪, ૧૨૦ (બી), ૪૦૬, ૪૨૦

આ ઉપરાંત આ બાબતે ઘણાંખરાં રાજ્યોમાં પણ અલાયદા કાયદા લાગુ પડે છે.

		
<p>નેહા એક મધ્યમ વર્ગ પરિવારમાં રહેતી હતી.</p>	<p>તે જીવનમાં તમામ વેલવી વસ્તુઓ મેળવવાની આકાંક્ષા ધરાવતી હતી.</p>	<p>તેને એક વેબસાઇટ મળી, જે BMW કાર, વિદેશ પ્રવાસ માત્ર રૂ. ૯૯૯૯માં ઉપલબ્ધ કરાવતી હતી.</p>
		
<p>તેણે તુરંત અપોઈન્ટમેન્ટ બુક કરાવી. તેને ફાઈવ સ્ટાર હોટેલમાં મુલાકાત માટે બોલાવવામાં આવી.</p>	<p>તેઓ જણાવે છે કે, જો તમારા દ્વારા બે સભ્ય કરવામાં આવશે તો તમને કમિશન પણ મળશે.</p>	<p>તે જેમ નવા લોકોને જોડશે તેમ તેના કમિશનમાં વધારો થશે તેમજ નવા લોકોનો સમાવેશ થશે.</p>
		
<p>શરૂઆતમાં તેને થોડું કમિશન પણ મળ્યું હતું. તેને પોતાના પૈસાથી પણ ઘણા બધા સભ્યોનો સમાવેશ કરાવ્યો.</p>	<p>એક દિવસ તે વેબસાઇટ બંધ થઈ ગઈ અને હેલ્પલાઇન નંબરો પણ. ન્યૂઝ મીડિયા પ્રમાણે ઓફર આપનાર લોકો ફોડ હતા.</p>	<p>નોંધાયેલા સભ્યો હવે તેના પાસે પૈસાની માંગ કરી રહ્યા હતા. તેને ઘણાં નાણાં અને સંબંધીઓનો વિશ્વાસ ગુમાવ્યો હતો. સાવધાન રહો.</p>

## ૧૭. મેટ્રીમોનીયલ વેબસાઈટ ફ્રોડ

છેતરપિંડી કરવાના ઈરાદાથી કોઈ વ્યક્તિ મેટ્રીમોનીયલ વેબસાઈટ પર નોંધણી કરાવી શકે છે. તેઓ પોતાની વિગત અને પ્રોફાઈલ ફોટોમાં પણ અન્ય વ્યક્તિની માહિતી આપી શકે છે. તેઓ ભોળી યુવતીઓને મીઠી વાતોથી મોહિત કરી શકે છે અને પોતાના પર વિશ્વાસ કેળવવા તે ખૂબ વાસ્તવિક લાગતી માહિતી આપી શકે છે. આ રીતે મેટ્રીમોનીયલ વેબસાઈટના માધ્યમથી ફ્રોડ થઈ શકે છે.

### લાગુ પડતી કલમો

ઈ.પી.કો. કલમ ૪૦૬, ૪૧૯, ૪૨૦, ૪૬૫

આઈ.ટી. એક્ટ કલમ ૬૬(સી), ૬૬ (ડી)

		
<p>ફાતિમા એન્જિનિયર તરીકે નોકરી કરતી હતી. તેનાં માતાપિતા તેના લગ્ન માટે યુવકની શોધમાં હતાં.</p>	<p>તેને લગ્નની અપેક્ષાએ ઘણી બધી મેટ્રીમોનીયલ સાઇટ્સ પર નોંધણી કરાવી હતી.</p>	<p>એક દિવસ તેને ૩૦ વર્ષના પુરુષ દ્વારા મેટ્રીમોનીયલ સાઇટ્સના માધ્યમથી ઈનબોક્ષમાં મેસેજ મળ્યો.</p>
		
<p>તે યુવક સરકારી નોકરી કરતો હતો અને પ્રતિષ્ઠિત કુટુંબ ધરાવતો હતો.</p>	<p>તેઓએ એકબીજાને મેસેજ મોકલવાનું શરૂ કર્યું અને પછી કોલ કરવાનું પણ. ફાતિમા તેને પસંદ કરવા લાગી હતી.</p>	<p>વિશ્વાસ કેળવવા માટે યુવકે પોતાનું નોકરીનું આઇડી કાર્ડ બતાવ્યું અને પરિવાર, મિત્રોની અંગત માહિતી પણ આપી હતી.</p>
		
<p>એક દિવસ યુવકે પોતાને નોકરીમાંથી સરપેન્ડ કરવામાં આવ્યો છે તેમ જણાવી, ફાતિમા પાસે નોકરી પાછી મેળવવા માટે ઉછીના પૈસા માંગ્યા હતા.</p>	<p>તેણે પોતાનો પાસપોર્ટ, આઇ.ડી., અને અન્ય દસ્તાવેજો સલામત રાખવા માટે ફાતિમાને આપ્યા. ફાતિમાએ તેને પાંચ લાખ રૂપિયા આપ્યા.</p>	<p>થોડા દિવસો પછી ફાતિમાને અખબારમાં થકી જાણ થઈ કે તે યુવકની મેટ્રીમોનીયલ માધ્યમથી યુવતીઓને છેતરવા બદલ ધરપકડ કરવામાં આવી છે.</p>

## ૧૮. મોબાઈલ રિપેર શોપ

તમારો ફોન જ્યારે અન્ય વ્યક્તિ પાસે હોય છે, ત્યારે તે વ્યક્તિ તમારા ફોનની ગેલેરીમાં સંગ્રહિત તસવીરો અને વીડિયો જોઈ શકે છે તેની કોપી પોતાની પાસે રાખી શકે છે. મોબાઈલ રિપેર શોપના માધ્યમથી જો તમારો ફોન ગુનાહિત માનસિકતા ધરાવનાર વ્યક્તિની પાસે પહોંચી જાય તો તે વ્યક્તિ તમારા અંગત ફોટો બદલરાદાથી વાઈરલ કરી શકે છે. તેને અયોગ્ય વેબસાઈટ્સ પર અપલોડ કરી શકે છે. તે તેનો ઉપયોગ તમને બ્લેકમેઈલ કરવા માટે પણ કરી શકે છે.

### લાગુ પડતી કલમો

આઈ.ટી. એક્ટ કલમ ૬૬





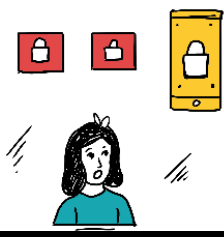

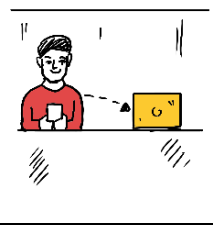
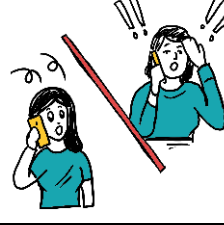

ઈ.પી.કો. કલમ ૪૦૬

**ઓનલાઈન પ્રસિદ્ધ કરવા બદલ લાગુ પડતી કલમો:-**

આઈ.ટી. એક્ટ કલમ ૬૭, ૬૭ (એ)

ઈ.પી.કો. કલમ ૫૦૬, ૫૦૭, ૫૦૮



		
<p>તન્વીને સેલ્ફી લેવાનું ખૂબ પસંદ હતું. તેની પાસે સારા કેમેરા સાથેનો ફ્લેગશિપ એન્ડ્રોઇડ ફોન હતો.</p>	<p>તે ફોનથી ઘણા ફોટો ક્લિક કરતી. તેણે ઘણા અંગત ફોટો પણ ક્લિક કર્યા હતા.</p>	<p>એક દિવસ તેનાથી ફોન આકસ્મિક રીતે નીચે પડી ગયો હતો. તેના ખૂબ પ્રયત્ન પછી પણ ફોન ચાલુ થયો નહીં.</p>
		
<p>ફોન રિપેર કરાવવા માટે તે ફોન કંપની દ્વારા માન્ય ના હોય તેવી નજીકની એક દુકાનને ગઈ હતી</p>	<p>તેને મનમાં હતું કે, તેના ફોટો અને અન્ય ડેટા સુરક્ષિત છે. કારણકે, તેણે પેટર્ન કોડ સાથે ફોન ગેલેરી સિક્યોર કરી હતી.</p>	<p>તે અજાણ હતા કે, પેટર્ન/પાસવોર્ડને હેકિંગ સોફ્ટવેરથી સરળતાથી તોડી શકાય છે.</p>
		
<p>ફોન રિપેર કર્યા પછી શોપકીપરે તેના મોબાઇલની ગેલેરી ઓપન કરી તેના ફોટો કોપી કરી લીધા હતા.</p>	<p>થોડા દિવસો પછી, તન્વીને તેના સંબંધી દ્વારા ફોન આવ્યો કે, તેના ફોટો વાઈરલ થયા હતા અને ઘણાં ઝૂપમા શેર કરવામાં આવ્યા હતા.</p>	<p>તન્વીને આવા ફોટો ક્લિક કરવા બદલ અફસોસ થાય છે હવે તે તેના પરિવાર અને સમાજનો સામનો કરવા માટે સંકોચ અનુભવતી હતી.</p>

## ૧૮. ફેક રિવ્યુઝ

ઈ-કોમર્સ વેબસાઈટ્સ તેઓની વેબસાઈટ પરની વસ્તુઓના ખોટા રિવ્યુઝ મુકીને ગ્રાહકો સાથે છેતરપિંડી કરી શકે છે. તેઓ ખૂબ આકર્ષક રિવ્યુઝ બતાવે છે, જેથી ગ્રાહક તે વસ્તુ ખરીદે છે, ખાસ કરીને આ વેબસાઈટ્સ ડિસ્કાઉન્ટેડ ભાવો આપે છે. શંકાસ્પદ સાઈટ્સનાં આ ઉત્પાદનોનો ઉપયોગ કરવાથી ઘણું નુકસાન થઈ શકે છે.

### લાગુ પડતી કલમો

ઈ.પી.કો. કલમ ૪૦૬, ૪૨૦

<p>નિકિતા એક શિક્ષિત યુવતી હતી. તે મોડેલ બનવા માંગતી હતી.</p>	<p>તે પ્રસિદ્ધિ માટે ઘણી પેજ ૩ પાર્ટીમાં હાજરી આપતી હતી.</p>	<p>તે મેક-અપ અને પરફ્યુમ્સ પાછળ પણ ખૂબ ખર્ચ કરતી હતી.</p>
<p>વધુ પાર્ટીમાં જવાના કારણે મેક-અપ અને પરફ્યુમ્સ માટે વધુ ખર્ચ થતો હોઈ તે કોસ્મેટિકના સરતા વિકલ્પની શોધમાં હતી.</p>	<p>૫૦% ડિસ્કાઉન્ટ પર તેની પસંદગીની કંપનીની પ્રોડક્ટ્સ ઓફર કરતી એક વેબસાઈટ તેના ધ્યાને આવી.</p>	<p>તેણે, આ ઓફર બરાબર ચકાસી, ગ્રાહકના રિવ્યુ પણ વાંચ્યા, વેબસાઈટને સરેરાશ ફોર સ્ટાર રેટિંગ મળ્યા હતા.</p>
<p>તેણે પરફ્યુમ્સ અને કોસ્મેટિક્સ ખરીદવાનું નક્કી કર્યું અને ઓનલાઇન ચુકવણી કરી હતી. ઓર્ડર કન્ફર્મેશન માટે તેને મેસેજ આવ્યો.</p>	<p>પ્રાપ્ત થયેલ આ પ્રોડક્ટ્સનો ઉપયોગ કરવાથી તેના ચહેરા પર ફોલીઓ તથા ચકામા પડી ગયા, જેનાથી ડરીને તે તુરંત હોસ્પિટલમાં દાખલ થઈ.</p>	<p>નિકિતા નક્કી રિવ્યુથી ગેરમાર્ગે દોરાઈ હતી. ઘણી વેબસાઈટ્સ આ પ્રકારે ખોટા રિવ્યુઝ પ્રસિદ્ધ કરે છે. તમે આ પ્રકારની વેબસાઈટ અને રિવ્યુઝથી છેતરાશો નહીં.</p>

## ૨૦. ફેક પ્રોફાઇલ અને સેક્ટોર્શન

શોપિંગ મોલ્સ/ અન્ય જાહેર સ્થળોના ચેન્જિંગ રૂમમાં ગુનાહિત ઉદ્દેશ સાથે અપરાધી દ્વારા વ્યૂહાત્મક રીતે કેમેરા મૂકવામાં આવી શકે છે, જે આ ચેન્જિંગ રૂમનો ઉપયોગ કરનાર વ્યક્તિની તસવીરો/ વીડિયો મેળવે છે. આ તસવીરો પછી ખંડણીના ઇરાદા સાથે ડુપ્લિકેટ સોશિયલ મીડિયા એકાઉન્ટ પર અપલોડ કરવામાં આવી શકે છે.

### લાગુ પડતી કલમો

તસવીર લેવી, વીડિયો કેપ્ચર કરવા બદલ લાગુ પડતી કલમો:-

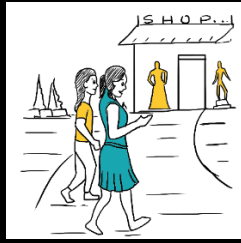
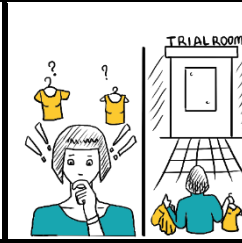
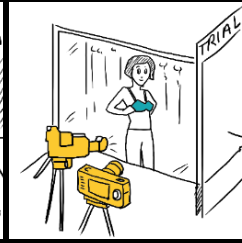

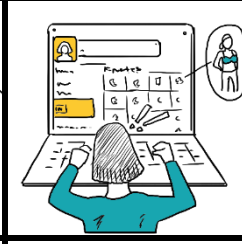
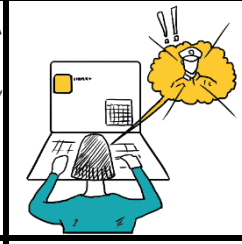

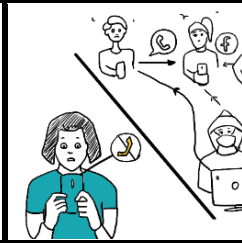
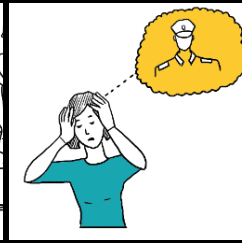
ઇ.પી.કો. કલમ ૩૫૪ (એ), ૩૫૪ (સી), ૪૧૯, ૫૦૭

આઇ.ટી. એક્ટ કલમ ૬૬ (સી)

ઓનલાઇન પ્રસિદ્ધ કરવા બદલ લાગુ પડતી કલમો:-

આઇ.ટી. એક્ટ કલમ ૬૭, ૬૭ (એ)

ઇ.પી.કો. કલમ ૫૦૯

		
<p>જહાન્વી તેના જન્મદિવસ માટે કપડાં ખરીદવા માંગતી હતી. તે તેના મિત્ર સાથે એક મોટી શોપમાં ગઈ હતી.</p>	<p>તેને ઘણાં કપડાં પસંદ આવતાં, પસંદ કરેલ તમામ કપડાં લઈને તે ટ્રાયલ રૂમમાં ગઈ.</p>	<p>તેને ખબર ન હતી કે, ચેન્જિંગ રૂમમાં બંને બાજુથી જોઈ શકાય તેવો અરીસો હતો અને બીજી બાજુ કેમેરા લગાવવામાં આવેલ હતા.</p>
		
<p>થોડા દિવસો પછી તેના મિત્રએ તેને ફોન કરી જણાવ્યું કે, શા કારણે તેણે અન્ય ફેસબુક એકાઉન્ટ બનાવ્યું?</p>	<p>મિત્રએ જણાવેલી પ્રોફાઇલ તપાસતા તેને આશ્ચર્ય થયું કે પ્રોફાઇલમાં તેનો જ ફોટો હતો, અને તેનો શોપમાં લેવાયેલ વીડિયો પણ તેમાં હતો.</p>	<p>તેણે તુરંત જ પ્રોફાઇલ રિપોર્ટ કર્યો પરંતુ સમાજમાં બદનામીના ડરથી તેણે પોલીસ ફરિયાદ કરી ન હતી.</p>
		
<p>થોડા દિવસો પછી તેને એક આંતરરાષ્ટ્રીય નંબર પરથી ઘમકીભર્યો કોલ આવ્યો, તેને રૂબરૂ મળવા બોલાવવામાં આવી હતી.</p>	<p>તેણે કોલરની અવગણના કરી. કોલરે તેના મિત્રો અને પરિવારને નકલી એકાઉન્ટ દ્વારા તેના ફોટો મોકલ્યા.</p>	<p>જહાન્વીએ હવે પોલીસને રિપોર્ટ કરવાનો નિર્ણય કર્યો, પરંતુ નુકસાન પહેલાં જ થઈ ચુક્યું હતું. આ બાબતે તમે પણ કાળજી રાખજો.</p>

## ૨૧. સાચબર ગીઢ્ઢ

સાચબર-વલ્ચર્સ (સાચબર ગીઢ્ઢ) ઁ ઁક પ્રકારના ઢેકર્સ ઁ, જૅઓ ખૂબ નિર્દયી ઢોય ઁ. જૅ ગીઢ્ઢની જૅમ અગાઉ ભોગ બનેલા અને નિરાશ થયેલા, માનસિક રીતે ઢારેલા, પડી ભાંગેલા લોકોને પોતાનો શિકાર બનાવે ઁ. આવા લોકોની પરિસ્થિતિ તથા માનસિક અવદશાનો લાભ લઈ ઢેકર્સ તેઓને વઘુ ઁતરે ઁ.

### લાગુ પડતી કલમો

આઈ.ટી. ઁક્ટ કલમ ૡૡ(સી), ૡૡ(ડી)

ઈ.પી.કો. કલમ ૧૨૦, ૡ૨૦

		
<p>મીસીઝ લોબો મધ્યમ વર્ગ પરિવારમાં રહેતી વિધવા મહિલા હતી. તેને બે પુત્રીઓ હતી.</p>	<p>તેમના સંબંધીએ તેમને બચત કરેલ રકમ ઉપર વધુ નફો કમાવવા માટે એક સ્કીમમાં રોકાણ કરવા સમજાવ્યું.</p>	<p>તેણે આકર્ષક જણાતી આ યોજનામાં તેના પતિના મૃત્યુ પછી તેને મળેલ વીમા રકમનું સંપૂર્ણ રોકાણ કર્યું.</p>
		
<p>એક દિવસ તેને જાણ થઈ કે, કંપનીના માલિક નાસી ગયા હતા અને તેણે તેના બધા પૈસા ગુમાવ્યા હતા.</p>	<p>એક હેકરે, કોઈ રીતે ઈન્વેસ્ટ કરેલા તમામ લોકોના ડેટાબેઝ તથા તેમને લગતી માહિતી મેળવી લીધી હતી.</p>	<p>હેકર રોકાણકારોને એક પછી એક કોલ કર્યો અને જણાવ્યું કે, જો તેઓ ૩૦% રૂપિયા એડવાન્સમાં આપશે, તો તે તેઓને પૈસા પાછા અપાવશે.</p>
		
<p>મીસીઝ લોબો ઓફર માટે સંમત થયા. હેકરે UPI કોડ, ATM પિન અને એકાઉન્ટ નંબર વગેરે વિગતો માંગી.</p>	<p>શ્રીમતી લોબોએ બચતના છેલ્લા બે લાખ રૂ. પણ હેકરને આપી દીધા. ફરી વાર છેતરાવા બદલ તેમને દુઃખ થયું.</p>	<p>તેના રૂપિયા અયોગ્ય કામગીરી સાથે સંકળાયેલ ઈ-વૉલેટ કંપનીના ખાતામાં ટ્રાન્સફર થયા હતા. અજાણ્યા કોલરથી સાવચેત રહે.</p>

## ૨૨. મોબાઈલ એપ્સ



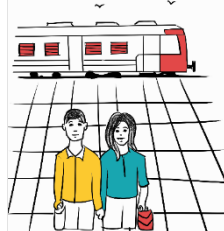


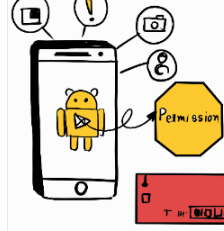
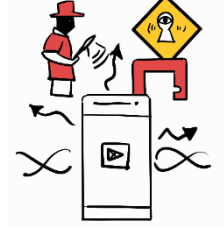

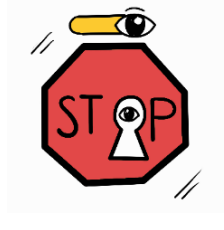
જ્યારે આપ મોબાઈલ એપ્સને વિવિધ ફાઈલ્સ, કેમેરા, માઈક્રોફોન્સ, વગેરેનો ઉપયોગ કરવાની પરવાનગી આપો છો ત્યારે આવી એપ્સ ઈન્ટરનેટના માધ્યમથી તમારી જાણ બહાર તમારા ડેટાને પોતાના સર્વર પર અપલોડ કરે છે. તમારા કેમેરા અને માઈક્રોફોન્સનો ઉપયોગ કરીને વીડિયો તથા તસવીરો લઈ શકે છે. અને ત્યારબાદ ખરાબ હેતુ અથવા અંગત ફાયદા માટે તેનો ઉપયોગ કરી શકે છે.

### લાગુ પડતી કલમો

આઈ.ટી. એક્ટ કલમ ૬૬

ઈ.પી.કો. કલમ ૪૦૬, ૪૨૦




		
<p>વિધા અને રોનક પાંચ વર્ષથી એકબીજાને પસંદ કરતાં હતાં. તેઓ ખૂબ સારા સંબંધ ધરાવતાં હતાં.</p>	<p>તેઓએ એક અઠવાડિયા માટે મનાલી ફરવા જવાનું નક્કી કર્યું હતું. સામાન તૈયાર કરી તેઓ રેલવે સ્ટેશને ગયાં.</p>	<p>મનાલીમાં ત્રણ અઢ્યુત દિવસો પસાર કર્યા પછી, તેઓ સારી યાદો સાથે પાછા ફર્યા.</p>
		
<p>વિધા એક એવી એપનો ઉપયોગ કરતી હતી કે, જે તેના હેલ્થ અને ફિટનેશ પર નજર રાખતી હતી.</p>	<p>આ મહિને વિધાને તબિયત ઠીક ન લાગતા તેને તે એપ સિવાય અન્ય એપ્લિકેશન્સ પણ ડાઉનલોડ કરી.</p>	<p>આપણા ફોનમાંની બીજી એપ્સની જેમ જ આ એપ્સે જીપીએસ, કોન્ટેક્ટ વિગત, અન્ય ડેટાનો ઉપયોગ કરવા માટે સંમતિ મેળવી લીધી.</p>
		
<p>વિધાને જાણ થઈ કે આ એપ્સ તેની હેલ્થ અને અન્ય માહિતી બીજી કંપનીઓને વેચતી હતી. વિધાને તેની અંગત માહિતી સુરક્ષિત ન હોવાનો અહેસાસ થયો.</p>	<p>આ એપ્સ તેની પરિસ્થિતિનો ફાયદો ઉઠાવીને તેનું પરીક્ષણ કરવા માટે તેની પાસે ચોક્કસ કિંમતની કિટની ખરીદવા માટે તેને જાહેરાત આપતી હતી.</p>	<p>આવી એપ્સ તમારો વીડિયો રેકોર્ડ કરી શકે તેમજ ડેટાને નિયંત્રિત કરી શકે છે. અંગત માહિતી અપલોડ/ ડાઉનલોડ કરી શકે છે. સાવચેતીપૂર્વક એપ્સ ડાઉનલોડ કરો.</p>

### રૂ૩. યાર્જિંગ પોઈન્ટ હેક

યાર્જિંગ સ્ટેશન પર સ્માર્ટફોન જેવાં ઉપકરણો યાર્જ કરવાથી તમારા ફોન હેક થઈ શકે છે. હેક કરવાની આ પદ્ધતિને જ્યુસ જેકિંગ કહે છે. જાહેર સ્થળોએ રાખવામાં આવેલ આ પ્રકારના યાર્જિંગ સ્ટેશનમાં યાર્જ કરવા માટેના કેબલમાં લોકોને દેખાય નહીં તે રીતે એક ચીપ લગાવેલ હોય છે, જે તમારા ફોનમાં માલવેર દાખલ કરી શકે છે, ફોન હેક કરી શકે છે અને જ્યારે ફોનની બેટરી યાર્જ થતી હોય તે સમય ગાળા દરમિયાન તે તમારો ડેટા પણ મેળવી લે છે.

### લાગુ પડતી કલમો

આઈ.ટી. એક્ટ કલમ ૬૬

		
<p>નિધિ એક વેકિંગ પ્લાનર, ઇવન્ટ ઓર્ગેનાઇઝર હતી. તેના જીવનમાં કામ જ સર્વસ્વ હતું.</p>	<p>તે ખાતરી કરતી હતી કે, તે દરેક લગ્ન કે જે તેણે આયોજન કર્યા હોય, તે ભૂલ વગરના હોય અને યાદગાર રહે.</p>	<p>નિધિ કર્મચારી/ કોન્ટ્રાક્ટરને બેવાર કોલ કરીને ખરાઈ કરતી હતી કે, બધી જ કામગીરી સારી રીતે થયેલ છે કે કેમ!</p>
		
<p>તેને કામ માટે ખૂબ મુસાફરી કરતા રહેવાનું થતું હતું. જેથી તેને ઘણી વાર એરપોર્ટ પર સમય પસાર કરવો પડતો.</p>	<p>તે ઘણી વાર ફોનમાં ચાર્જિંગ કરવા માટે એરપોર્ટ પર ઉપલબ્ધ ચાર્જિંગ સ્ટેશન્સનો ઉપયોગ કરતી.</p>	<p>તેને અનુભવાય છે કે, તેનો ફોન ધીમો થઈ ગયો હતો અને સતત વપરાશમાં હોય ત્યારે ઝડપથી ગરમ થતો હતો.</p>
		
<p>એન્ટિ વાઇરસ દ્વારા ફોન સ્કેન કરતા જોખમી વાઇરસની ફોનમાં હાજરી હોવાની જાણ થઈ, જેથી ફોનની ઝડપમાં ઘટાડો થયો હતો.</p>	<p>એરપોર્ટ પરના કીઓસ્ક ચાર્જિંગ મશીન પરથી ફોન ચાર્જ કરવા દરમિયાન માલવેર ફોનમાં દાખલ થયો હતો.</p>	<p>જ્યુસ જેકિંગ દ્વારા ફોનમાંથી ગુપ્ત ફોટો અને વીડિયો ચોરાયા હતા. તમે કાળજી રાખજો.</p>


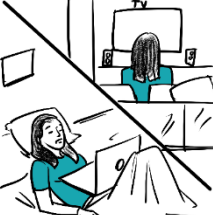







## ૨૪. વાઈફાઈ હેક

હેકર્સ તમારા વાઈફાઈ નેટવર્કમાં લોગઈન કરીને પોતાનું ડિવાઈઝ કનેક્ટ કરે છે. જેનો ઉપયોગ કરીને તે નેટવર્કમાં કનેક્ટેડ અન્ય ડિવાઈઝના ડેટા/ ફાઈલ્સનો ઉપયોગ કરી શકે છે. ઈન્ટરનેટ પર અયોગ્ય ફાઈલ્સ ડાઉનલોડ/અપલોડ કરી શકે છે. તમારા દ્વારા વાઈફાઈ નેટવર્કનો સરળ પાસવર્ડ્સ રાખવાથી આ પ્રકારના હેકિંગનો ભોગ બનવાની શક્યતા ખૂબ વધી જાય છે.

### લાગુ પડતી કલમો

આઈ.ટી. એક્ટ કલમ ૬૬, ૬૬(સી), ૬૬(ડી)

ઈ.પી.કો. કલમ ૪૧૯, ૪૨૦

		
<p>દિવ્યાને ફિલ્મ જોવાનો ખૂબ શોખ હતો. તે નેટફ્લિક્સ પર દરરોજ બે મૂવિઝ જોવા ટેવાયેલી હતી.</p>	<p>તે તેના લિવિંગ રૂમના સ્માર્ટ ટીવી અથવા બેડરૂમમાં તેપટોપથી હંમેશાં ફિલ્મ જોતી હતી.</p>	<p>તેણે રોજના પાંચ GB ઇન્ટરનેટ આપતું પ્રોડબેન્ડ કનેક્શન લીધું હતું. જેમાંથી માંડ એક GB બાકી રહેતું.</p>
		
<p>તે જે રૂમમાં રહેતી હતી ત્યાં તેણે વાઈફાઈ રાઉટર લગાવ્યું. તેનું સિગ્નલ સારુ હોવાથી બધા રૂમથી કનેક્ટ કરી શકાતું હતું.</p>	<p>એક દિવસ, તેણે જોયું કે, ઇન્ટરનેટ સ્પીડ ધીમી હોવાને કારણે ફિલ્મ અટકીને ચાલતી હતી.</p>	<p>તેણે તેના લેપટોપને તપાસ્યું કે પાછળ બીજી કોઈ ફાઈલ્સ ડાઉનલોડ થઈ રહી છે કે શુ!</p>
		
<p>તે તેના રાઉટરના એડમિન પેનલમાં લોગ ઇન કરીને જોયે છે, તો તેને જાણ થાય છે કે, અન્ય ડિવાઈઝ પણ નેટવર્કમાં કનેક્ટેડ હતી.</p>	<p>તપાસ કરતા જાણ થાય છે કે, તેના સરળ અને નબળા પાસવર્ડના લીધે, કોઈએ તેનું વાઈફાઈ હેક કરી, નેટવર્કમાં પ્રવેશ કરેલ હતો.</p>	<p>પાછળથી તેને જાણવા મળે છે, તેઓ ખરાબ લોકો હતા અને તેઓએ તેના ઇન્ટરનેટનો ઉપયોગ કરીને ડાર્ક વેબ પર ડ્રગ્સ અને અયોગ્ય વસ્તુઓ વેચી હતી.</p>

## ૨૫. ઓનલાઈન કટ્ટરવાદ ફેલાવવો

યુવાન, સંવેદનશીલ વ્યક્તિઓ ઓનલાઈન સમય પસાર કરતા અને નેટ બ્રાઉઝ કરતી વખતે આતંકવાદીઓના પ્રચારનો શિકાર બની શકે છે. આવા ઉગ્રવાદીઓનું લક્ષ્ય વ્યક્તિઓ અથવા લોકોના દિલ-દિમાગમાં આતંકવાદી વિચારો દાખલ કરવાનો હોય છે. આ રીતે તેઓ નિર્દોષ અને ભોળા લોકોને આતંકવાદી પ્રવૃત્તિ કરવા દુષ્પ્રેરણા આપે છે.

### લાગુ પડતી કલમો

આઈ.ટી. એક્ટ કલમ ૬૬(એફ)

ઈ.પી.કો. કલમ ૧૨૦ (બી), ૧૨૧, ૧૨૧(એ), ૧૨૨,  
૧૨૪(એ)

		
<p>રેશમા એક સરળ યુવતી હતી. તેણે એન્જિનિયરિંગમાં અભ્યાસ કર્યો હતો.</p>	<p>તેનાં માતાપિતા ઈચ્છતા ન હતા કે, તે નોકરી કરે. તેઓએ આફ્રિકામાં નોકરી કરતા યુવક સાથે તેનાં લગ્ન કરાવી દીધાં.</p>	<p>તેના પતિ તેને લગ્ન બાદ પોતાના સાથે આફ્રિકા લઈ ગયા હતા.</p>
		
<p>તે ક્યાંય પણ ફરવા ન જતી. તે આખો દિવસ ઘરે રહેતી, અને મોટા ભાગનો સમય ઓનલાઇન પસાર કરતી.</p>	<p>એકવાર તેણે વેબસાઇટ પર એક પોસ્ટ જોઈ અને ત્યાં ક્લિક કરતા તે વિચિત્ર ફોટો અને પોસ્ટ્સ ધરાવતી એક વેબસાઇટ પર પહોંચી.</p>	<p>તેને વેબસાઇટ પરથી ઈ-મેઇલ મળ્યો અને ધીમે ધીમે વેબસાઇટના માલિક સાથે તેની નિયમિત વાતચીત શરૂ થઈ.</p>
		
<p>તેઓએ રેશમાના દિમાગમાં ઉગ્રવાદી વિચારધારા ભરી દીધી હતી. તેના ઘરે હથિયારો પણ પહોંચાડ્યાં.</p>	<p>બીજા દિવસે તેણે એક મોલમાં પ્રવેશે કર્યો અને સ્વર્ગ મેળવવાની લાલશામાં આત્મઘાતી હુમલો કર્યો.</p>	<p>રેશમા કટ્ટરપંથી લોકોના સંપર્કમાં હતી, જે બાબતે તેના પતિ અને પરિવારના લોકો અજાણ હતા. તેઓ ભાંગી પડ્યા હતા.</p>

## ૨૬. હની ટ્રેપ






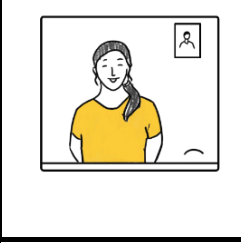


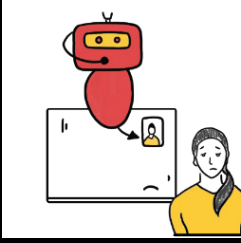
ફોડ કરનાર વ્યક્તિ દ્વારા આપના સાથે વ્યક્તિગત રીતે ઘનિષ્ઠ સંબંધો કેળવવામાં આવે છે અને ત્યાર બાદ આપનો વિશ્વાસ કેળવીને આપની અંગત વિગતો મેળવીને, ફોટો/વીડિયો કેપ્ચર કરીને આપને બ્લેકમેઇલ કરવામાં આવે છે. આ પ્રકારના ફોડને હની ટ્રેપ કહે છે.

## લાગુ પડતી કલમો

ઇ.પી.કો. કલમ ૩૫૪(સી), ૩૮૪, ૫૦૯

આઇ.ટી. એક્ટ કલમ ૬૬(ઇ), ૬૭, ૬૭(એ)



		
<p>સુમા દુઃખી પારિવારિક જીવન જીવતી એક વિવાહિત સ્ત્રી હતી.</p>	<p>તે સૂતા પહેલાં દરરોજ પોતાના લેપટોપમાં કોઈ અજાણી વ્યક્તિ સાથે વીડિયો ચેટ કરવા ટેવાયેલી હતી.</p>	<p>એક રાત્રે તે એક મોહન નામની સુંદર વ્યક્તિ સાથે ચેટ કરતી હતી.</p>
		
<p>મોહને એક દિવસ તેને વીડિયો કોલથી વાત કરવા જણાવ્યું, સુમાએ ઉત્સાહિત થઈને વીડિયો કોલ કર્યો</p>	<p>મોહને એક પછી એક પોતાનાં કપડાં ઉતારવાનું ચાલુ કર્યું અને થોડા સમય બાદ સુમાને પોતાનાં કપડાં ઉતારવા કહ્યું.</p>	<p>સુમાએ પણ ખુશીથી પોતાનાં કપડાં ઉતાર્યાં અને ટૂંક સમયમાં ચેટ પુર્ણ થઈ.</p>
		
<p>થોડા જ સમયમાં સુમાને વેબ કેમેરા દ્વારા ઉતારેલ પોતાનો બીભત્સ જણાતો વીડિયો ઈ-મેઇલ દ્વારા મળ્યો. તેઓ ખંડણીની માંગ કરતા હતા.</p>	<p>જો તે રૂપિયાની ચુકવણી નહીં કરે તો વીડિયો વાઈરલ થશે અને તેનું કુટુંબ જોશે તેવા ડરથી સુમા ગભરાઈ ગઈ હતી.</p>	<p>તે અજાણ હતી કે, તે એક AIથી બનાવેલું ચેટ બોટ સાથે વાત કરતી હતી. અને તેમાં પ્રી-રેકોર્ડેડ વીડિયો હતો. ઠેકર દ્વારા તેને ફસાવવામાં આવી હતી.</p>

## ૨૭. QR કોડ

QR (કિવક રિસ્પોન્સ) કોડ બારકોડની જેમ એક કોડ છે. જેને સ્કેન કરીને તમે અન્ય વ્યક્તિને UPI પેમેન્ટ એપ્સથી નાણાં ચૂકવી શકો છો. ફોડ કરવાના ઈરાદાથી અન્ય વ્યક્તિ આપને નાણાં મેળવવા માટે QR Code સ્કેન કરવા જણાવે છે. આપ અજાણતા કોડ સ્કેન કરીને નાણાં મેળવી રહ્યાં છો તેમ સમજીને ભુલમાં જે તે વ્યક્તિને નાણાં ચૂકવો છો.

### લાગુ પડતી કલમો

ઈ.પી.કો. કલમ ૪૦૬, ૪૨૦

આઈ.ટી. એક્ટ કલમ ૬૬ (સી), ૬૬ (ડી)

		
<p>કોમલ એકલી રહેતી હતી. તેનાં બંને સંતાનો વિદેશ રહેતાં હતાં. તે ઘણાખરું કામ ફોનથી કરવાનું શીખતી હતી.</p>	<p>તાજેતરમાં તેણે પોતાનો જૂનો મોબાઇલ ફોન વેચવા માટે OLX ઉપર જાહેરાત મૂકેલ હતી.</p>	<p>આમી ઓફિસર તરીકે ઓળખ આપનાર એક વ્યક્તિએ તે ફોન ખરીદવાની ઈચ્છા વ્યક્ત કરી, તેનો સંપર્ક કર્યો.</p>
		
<p>તે વ્યક્તિએ કોમલના વિશ્વાસ માટે પોતાનું આઇકાર્ડ દેખાડ્યું, આમી તરીકેની ફરજ સંબંધિત અનુભવો વર્ણવ્યા.</p>	<p>વિશ્વાસ કેળવ્યા બાદ તેણે કોમલને પોતાનો QR કોડ મોકલ્યો. નાણાં રિસિવ કરવા માટે કોડ સ્કેન કરવા જણાવ્યું.</p>	<p>કોમલ, તેના જણાવ્યા મુજબ QR કોડ સ્કેન કરીને નાણાં મેળવવા માટે ૧૭,૦૦૦ રકમ દાખલ કરીને PIN નંબર દાખલ કર્યો.</p>
		
<p>તરત જ તેને બેન્ક તરફથી પોતાના એકાઉન્ટમાંથી રૂ. ૧૭,૦૦૦ અન્યને ચૂકવાયા હોવાનો મેસેજ પ્રાપ્ત થયો.</p>	<p>ટેકનિકલ ખામીના કારણે પૈસા કપાયા હશે અને ૧૦ દિન બાદ પરત મળી જશે તેમ જણાવી તે વ્યક્તિએ ફરી રૂપિયા મેળવવા માટે કાર્યવાહી કરવા જણાવ્યું.</p>	<p>પુનઃ પ્રક્રિયા કરતા બીજાવાર પણ નાણાં ચૂકવાયા હોવાનું તેને લાન થાય છે અને પોતે છેતરાઈ ગઈ હોવાનો અહેસાસ થયો. તમે છેતરાશો નહીં.</p>




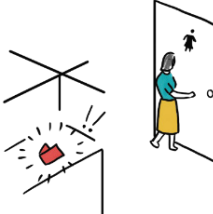





## ૨૮. RFID ક્લોનિંગ

Radio Frequency Identification (RFID) ટેગ એ એક બારકોડ જેમ જ સ્કેન કરવા માટેનો ટેગ છે. આવા પ્રકારના ટેગ પ્રથમ વ્યક્તિ અથવા વસ્તુને ફાળવવામાં આવે છે. ત્યારબાદ કોડ રીડ કરવાના મશીનથી સ્કેન કરતાં મશીન દ્વારા તે વ્યક્તિ/વસ્તુની માહિતી રીડ કરી શકાય છે. આ પ્રકારના ટેગનો અન્ય વ્યક્તિ દ્વારા દુરુપયોગ થઈ શકે છે.

### લાગુ પડતી કલમો

આઈ.ટી. એક્ટ કલમ ૬૬, ૬૬(બી), ૬૬(સી), ૬૬(ડી)

ઈ.પી.કો. કલમ ૪૧૯, ૪૨૦










		
<p>આઈશા IT વલ્લાગમાં કામ કરતી કંપનીની ઓફિસમાં પ્રવેશ કરવા માટે તે પોતાના RFID ટેગનો ઉપયોગ કરતી.</p>	<p>તે તેના પર્સમાં RFID કાર્ડ રાખતી અને સ્કેન કરવા માટે પોતાનું પર્સ RFID કાર્ડ રીડર સામે રાખતી.</p>	<p>આદત મુજબ પોતાનું પર્સ હંમેશાં પોતાના ટેબલ પર રાખતી.</p>
		
<p>એક દિવસ જ્યારે આઈશા પોશરૂમમાં ગઈ ત્યારે રોજની જેમ પોતાનું પર્સ ડેસ્ક ઉપર રાખીને ગઈ હતી.</p>	<p>તેનો એક મિત્ર જોન કે જેને આઈશાની સફળતાથી ઈર્ષ્યા થતી હતી. તેણે તેનું RFID કાર્ડ, રીડરથી સ્કેન કર્યું.</p>	<p>જોને આઈશાના પર્સમાંથી ઓફિસ આઈડીકાર્ડ ઉપરાંત ક્રેડિટ કાર્ડની માહિતી મેળવી લીધી હતી.</p>
		
<p>જોને રૂપિયા મેળવવા માટે આઈશાના ક્રેડિટ કાર્ડની માહિતી ડાર્કવેબ પર વેચી હતી.</p>	<p>જોને આઈશાની માહિતીનો ઉપયોગ કરી તેનું ડુપ્લિકેટ ઓફિસ આઈડીકાર્ડ બનાવેલ હતું.</p>	<p>જોને આ ડુપ્લિકેટ આઈડીનો ઉપયોગ કરીને સર્વર રૂમમાં પ્રવેશ કર્યો અને બાદમાં સીસ્ટમ હેક કરી જેના માટે આઈશાને જવાબદાર ઠેરવવામાં આવી.</p>

## ૨૯. ડ્રોન સર્વેક્ષણ

એવીએશન (ઉડ્ડયન) ક્ષેત્રમાં પાઈલટ વગર ઊડી શકે તેવા ઉપકરણને ડ્રોન કહે છે. ડ્રોનમાં સર્વેક્ષણ કરી શકાય તે માટેનાં ઉપકરણો લગાવેલ હોઈ શકે જેથી તેનો ઉપયોગ વીડિયો/તસવીરો લેવા માટે થઈ શકે છે. આવા ઉપકરણમાં અન્ય વિવિધ ટેકનોલોજીનાં સંસાધનો લગાવીને ડ્રોનનો ઉપયોગ કોલ ઈન્ટરસેપ્ટ કરવા, GPS લોકેશન મેળવવા લાઈસન્સ પ્લેટ ઓળખવા માટે કરી શકાય છે.

### લાગુ પડતી કલમો

ઈ.પી.કો. કલમ ૩૫૪ (એ), ૩૫૪ (સી), ૩૫૪ (ડી),  
૫૦૯  
આઈ.ટી. એક્ટ કલમ ૬૬ (ઈ)

		
<p>અનુરાઘા મેડિકલમાં અભ્યાસ કરતી હતી. બિલ્ડિંગના તેત્રીસમાં માણે તેનું ઘર હતુ. બિલ્ડિંગ ઘણી ઊંચી હતી.</p>	<p>તેના ઘરની આસપાસ અન્ય ઘર પણ ન હતું. તેથી તે ઘરની બારીઓ હંમેશાં ખુલ્લી રાખતી હતી.</p>	<p>અનુરાઘાને ઓછામાં ઓછા કપડાં પહેરીને ઘરમાં ફરવાની ટેવ હતી. તે ઘરમાં એકલી રહેતી હતી.</p>
		
<p>તેનો ભૂતપૂર્વ બોયફ્રેન્ડ અક્ષય ડ્રોનનો ઉપયોગ અનુરાઘા પર નજર રાખવા કરતો હતો.</p>	<p>તે ડ્રોનના ઉપયોગથી અનુરાઘાના બેડરૂમ અને લિવિંગ રૂમનો છૂપીરીતે વીડિયો બનાવતો.</p>	<p>તે ડ્રોનનો ઉપયોગ તેના ઘરની અંદર અને બહારની હિલચાલ પર નજર રાખવા કરતો હતો.</p>
		
<p>ડ્રોનમાં વાઈફાઈ કેકર પણ રાખવામાં આવેલ, જેનાથી તેનો તમામ ઓનલાઈન ડેટા મેળવવામાં આવેલ.</p>	<p>ડ્રોનનો ઉપયોગ કરીને અક્ષય તેના ઘરમાં હાનિકારક મટીરિયલ્સ અને હથિયાર પણ મોકલી શકતો.</p>	<p>તેણે જો શરૂઆતમાં મોશન સેન્સર સાથેના સીસીટીવી કેમેરા લગાવેલ હોત, તો તે ડ્રોનને ટ્રેક કરી શકત.</p>

### ૩૦. ગુગલ સર્ચ




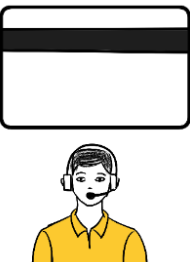



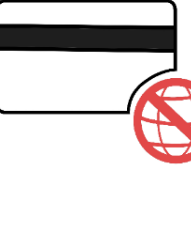
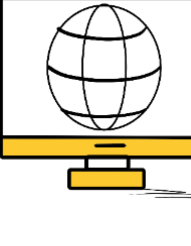
હેકર્સ દ્વારા વાસ્તવિક લાગતી વેબસાઈટ જેવી જ વેબસાઈટ બનાવવામાં આવે છે અને તેને પ્રસિદ્ધ કરવામાં આવે છે. હેકર્સ દ્વારા વિવિધ વેબસાઈટ્સ/વેબપેજ ઉપર ગેરમાર્ગે દોરતી માહિતી પ્રસિદ્ધ કરવામાં આવે છે અથવા ખોટા હેલ્પલાઈન નંબર પ્રસિદ્ધ કરવામાં આવે છે અને ત્યારબાદ સર્ચ એન્જિન ઓપ્ટિમાઇઝેશન અલ્ગોરિધમને એ રીતે ગેરમાર્ગે દોરવામાં આવે છે કે, જેથી તેઓએ પ્રસિદ્ધ કરેલ માહિતી સર્ચ એન્જિનનો ઉપયોગ કરનાર વ્યક્તિને પ્રથમ દેખાય છે અને આ રીતે લોકો સાથે ગેરરીતિ આચરવામાં આવે છે.

### લાગુ પડતી કલમો

આઈ.ટી. એક્ટ કલમ ૬૬(સી), ૬૬(ડી)

ઈ.પી.કો. કલમ ૪૧૯, ૪૨૦



		
<p>અક્ષતાએ ગોવા જવા ફ્લાઈટની ટિકિટ બુક કરાવી હતી.</p>	<p>મુસાફરીના બે દિવસ પહેલા તેને ઈ-મેઈલ મળેલ કે, તેની ટિકિટ કેન્સલ થયેલ છે.</p>	<p>તેણે ગુગલ પર સર્ચ કરીને હેલ્પલાઈન નંબર મેળવી તેમને ફોન કર્યો.</p>
		
<p>કસ્ટમર કેર તરફથી વાત કરનારે, વેરિફિકેશન માટે ડેબિટ કાર્ડની માહિતી અક્ષતાને પૂછેલ.</p>	<p>તુરંત તેને રૂ. ૧૦,૦૦૦ તેના એકાઉન્ટમાંથી સતત પાંચ વખત ડેબિટ થયાનો મેસેજ આવ્યો. (કુલ રૂ. ૫૦,૦૦૦)</p>	<p>જે ઈ-મેઈલ તેને મળ્યો હતો, તે એરલાઈન કંપનીનો નહીં પરંતુ બનાવટી હતો.</p>
		
<p>ગુગલ પર સર્ચ કરતા મળતા હેલ્પલાઈન નંબરો ગુનેગાર દ્વારા વેબસાઈટ પર અપલોડ કરેલ હોય છે. આ રીતે તેઓ લોકોને ફસાવતા હોય છે.</p>	<p>અક્ષતાએ કોઈ ઓટીપી આપ્યો ન હતો, પરંતુ તેને અંદાજ ન હતો કે, વિદેશમાં ટ્રાન્ઝેક્શન કરવા માટે ઓટીપીની જરૂર પડતી નથી.</p>	<p>અક્ષતાએ તેના ક્રેડિટ કાર્ડ અને ડેબિટ કાર્ડ પર આંતરરાષ્ટ્રીય ઉપયોગ કરવા માટેનો ઓપ્શન ડિસેબલ કરેલ ન હતો.</p>

### ૩૧. IDN હોમોગ્રાફ એટેક

IDN હોમોગ્રાફ એટેક એ એક પ્રકારનો સાચબર એટેક છે, જેમાં ગેરરીતિ આચરનાર વ્યક્તિ દ્વારા વાસ્તવિક લાગતી વેબસાઈટ જેવી જ વેબસાઈટ બનાવવામાં આવે છે અને તે વેબસાઈટનું એક્સેસ પણ વાસ્તવિક વેબસાઈટના નામ જેવું જ લાગે તેવું નામ આપવામાં આવે છે, જેથી ભોગ બનનાર વ્યક્તિ દ્વારા આ વેબસાઈટ અજાણતા જ, વાસ્તવિક વેબસાઈટ છે તેમ સમજીને ઉપયોગ કરવામાં આવે છે. તેમાં પોતાની અંગત માહિતી અથવા લોગઈન વિગત દાખલ કરવામાં આવે છે. જેનો ઉપયોગ કરીને ગેરરીતિ આચરવામાં આવે છે.

#### લાગુ પડતી કલમો

આઈ.ટી. એક્ટ કલમ ૬૬(સી), ૬૬(ડી)

ઈ.પી.કો. કલમ ૪૧૯, ૪૨૦

<p>સુચેતા તેની માતાને પેસા મોકલવા ઈચ્છતી હતી. તેની માતા અન્ય શહેરમાં રહેતી હતી.</p>	<p>તેને તેની બેન્કમાંથી એક મેસેજ (સંદેશ) આવ્યો હતો.</p>	<p>જે મેસેજ ખોલતા તેને બેન્કમાંથી ગિફ્ટ વાઉચર મળ્યાં હોવાની જાણ થયેલ.</p>
<p>ઉત્સાહિત થઈ તેણે મેસેજમાં આપેલ બેન્કની લિંક પર લોગ ઈન થવા માટે યુઝર આઈડી તથા પાસવર્ડ દાખલ કરેલ.</p>	<p>પોતાની લોગઈન વિગત આપ્યા પછી પણ તે લોગ ઈન થઈ શકતી નથી, તેના બદલે તેને ફરીથી લોગઈન પેજ જોવા મળ્યું હતું.</p>	<p>તેણે ફરીથી એકવાર પોતાના યુઝર આઈડી તથા પાસવર્ડ દાખલ કરેલ અને સફળતાપૂર્વક લોગઈન થયેલ.</p>
<p>ગિફ્ટ વાઉચરની જગ્યાએ, તેને તેના ખાતામાંથી રૂ. ૧૦,૦૦૦ કપાઈ ગયા હોવાનું ધ્યાને આવતા તે અચંબિત થઈ ગઈ હતી.</p>	<p>સુચેતા IDN હોમોગ્રાફનો ભોગ બની હતી, જેમાં નકલી ડોમેઈન્સનો ઉપયોગ કરી વાર્તાવિક લાગતી વેબસાઈટ બનાવવામાં આવે છે.</p>	<p>તેણે તેના બ્રાઉઝરને અપડેટ કર્યા હોત તો તેને બનાવટી વેબસાઈટ અને ડોમેઈન અંગે ચેતવણી મળી હોત.</p>




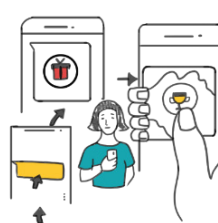



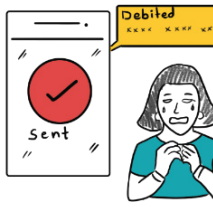
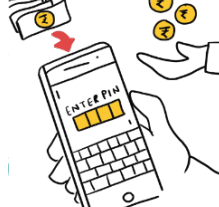
### ૩૨. સ્કેચકાર્ડ

ગેરરીતિ આચરનાર વ્યક્તિ દ્વારા પેમેન્ટ વોલેટ દ્વારા સ્કેચકાર્ડ પાઠવવામાં આવે છે, તે જ પ્રકારનું સ્કેચકાર્ડ આપને મળેલ છે તેવું કોઈની કોઈ વેબસાઈટ અથવા મેસેજ કે અન્ય માધ્યમથી આપને જણાવવામાં આવે છે, જેના પર ઈનામ મેળવવાની અથવા કેશબેક મેળવવાની લાલચમાં ભોળવાઈને આપના સાથે છેતરપિંડી આચરવામાં આવે છે.

#### લાગુ પડતી કલમો

આઈ.ટી. એક્ટ કલમ ૬૬(સી), ૬૬(ડી)

ઈ.પી.કો. કલમ ૪૧૯, ૪૨૦

		
<p>અમરીનને રૂ. બે લાખની ખૂબ જરૂર હતી. તે ખૂબ જ ચિંતિત હતી.</p>	<p>તેણે ભગવાનને પ્રાર્થના કરી, તે હવે કોઈ ચમત્કારની અપેક્ષા રાખતી હતી.</p>	<p>તેણે અચાનક એક વોટ્સએપ ગ્રૂપમાંથી પાંચ લાખ સુધીની રકમ જીતવા માટે એક સ્કેચકાર્ડ મળ્યું.</p>
		
<p>અમરીને લિંક પર ક્લિક કરી પ્રાપ્ત થયેલ કાર્ડને આતુરતાથી સ્કેચ કર્યું.</p>	<p>તે રૂપિયા ત્રીસ હજાર જીતી હતી અને એ માટે તેણે ભગવાનનો આભાર માન્યો.</p>	<p>વોલેટ એપ ખૂલતા તેણે તુરંત પૈસા મેળવવા માટે પોતાનો પિન નંબર દાખલ કર્યો હતો.</p>
		
<p>અહીં આ ટ્રાન્ઝેક્શન પૈસા મેળવવા માટે નહીં, પરંતુ ચુકવણી માટે હતું, જે અમરીનને ખબર ન હતી.</p>	<p>અમરીને મહેનતથી કમાયેલા રૂ. ૩૦,૦૦૦ ગુમાવ્યા હતા.</p>	<p>યાદ રાખો, વોલેટમાં પૈસા મેળવવાના હોય ત્યારે પિન નંબર દાખલ કરવાનો રહેતો નથી.</p>

### ૩૩. સીમ સ્વેપ

છેતરપિંડી કરવાના ઈરાદાથી ગુનેગાર દ્વારા ટેલીકોમ સર્વિસ પ્રોવાઈડર તરફથી આપવામાં આવતી મોબાઈલ નંબર પોર્ટેબીલીટી જેવી સુવિધાનો દુરુપયોગ કરવામાં આવે છે. તેઓ દ્વારા તમારા ફોન નંબરને પોર્ટ કરીને, નંબરનો સંપુર્ણ એક્સેસ મેળવી લેવામાં આવે છે. આપના નંબર સાથે અન્ય પેમેન્ટ એપ્સ, આધાર નંબર સેવા, બેન્ક સેવા, સોશિયલ મીડિયા એકાઉન્ટ વગેરે જોડાયેલ હોય છે જેનો ત્યારબાદ બદલવાથી ઉપયોગ કરવામાં આવે છે. આ પ્રકારની ગેરરીતિ આપનો ફોન ચોરાઈ/ખોવાઈ જાય છે ત્યારે અથવા આપના દ્વારા અન્ય સર્વિસ પ્રોવાઈડરમાં સેવાઓ ટ્રાન્સફર કરવાનો પ્રયત્ન કરવામાં આવે ત્યારે આચરવામાં આવે છે. આ પ્રકારના ફોનને પોર્ટ આઉટ સ્કેમ, સીમ સ્પીલીટીંગ, સીમ સ્વેપિંગ, સ્મિશિંગ અને સીમ જેકિંગ પણ કહે છે.

### લાગુ પડતી કલમો

આઈ.ટી. એક્ટ કલમ ૬૬, ૬૬(સી), ૬૬(ડી)

ઈ.પી.કો. કલમ ૪૧૯, ૪૨૦

<p>અર્પિતા મોબાઇલ ફોનનો ખૂલ ઉપયોગ કરતી હતી. તે તમામ એપ્સમાં લોગઇન થવા માટે તેના મોબાઇલ નંબરનો ઉપયોગ કરતી હતી.</p>	<p>તેના મોબાઇલમાં વોલેટ, ઇ-મેઇલ, બેન્ક એકાઉન્ટ્સ, સોશિયલ મીડિયા વગેરે માટેની એપ્સ હતી.</p>	<p>એક રાત્રિએ અર્પિતાને એક સાયબર ક્રિમીનલ તરફથી ફોન આવ્યો. તેણે સેલ ફોન કંપનીના પ્રતિનિધિ તરીકે પોતાની ઓળખ આપી હતી.</p>
<p>તે માત્ર મર્યાદિત ગ્રાહકો માટે એક 5G એક્ટિવેશન બોનસ ઉપલબ્ધ કરાવી રહ્યા હતા. જેના માટે પોતાનો ફોન બે કલાક બંધ રાખવાનો હતો.</p>	<p>અર્પિતા તેના ફોનને બંધ (સ્પીચ ઓફ) કરી સૂઈ ગઈ હતી અને જ્યારે તે સવારે ઊઠી હતી ત્યારે તેના ફોન પર કોઈ નેટવર્ક આવતું ન હતું.</p>	<p>હેકરે તેના આઈડીકાર્ડની મદદથી, તેનું નવું સીમ કાર્ડ મેળવી લીધું હતું. નવું કાર્ડ સક્રિય થતાંની સાથે જ જૂનું કાર્ડ બંધ થઈ ગયું હતું.</p>
<p>ફોર્ગેટ પાસવર્ડ અને ઓટીપી વેરિફિકેશન વિકલ્પનો ઉપયોગ કરીને હેકરે તેના તમામ એકાઉન્ટ્સનું નિયંત્રણ મેળવી લીધું હતું. જે અર્પિતાને ખબર ન હતી.</p>	<p>હેકરે અર્પિતાના વોટ્સએપનું નિયંત્રણ મેળવી લીધું હતું અને તેની ખાનગી ચેટ્સ /ફોટો વગેરે અર્પિતાને બ્લેકમેઇલ કરવા માટે વાપર્યાં.</p>	<p>હેકરે સીમ સ્વેપ કર્યા વગર પણ વિશિંગ, ક્રિશિંગ, સ્મિશિંગ વગેરે દ્વારા ઓટીપી મેળવી વોટ્સએપ તથા અન્ય એકાઉન્ટ્સ હેક કરે છે.</p>

### ૩૪. ક્લિપ્ટો જેકિંગ




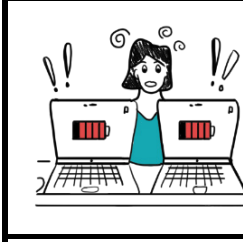
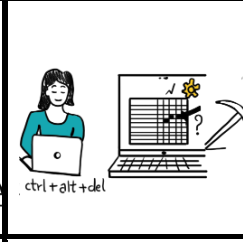

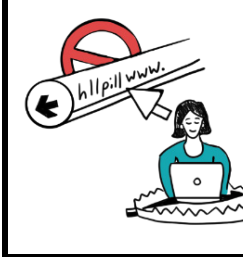
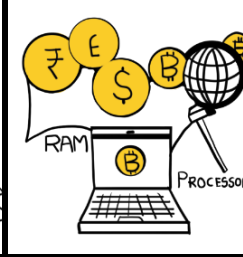

ગેરરીતિ આચરનાર વ્યકિત દ્વારા આપના કમ્પ્યૂટર ઉપકરણની કમ્પ્યૂટેશન (કામ કરવાની) ક્ષમતાનો ઉપયોગ ક્લિપ્ટો માઈનિંગ કરવા માટે વાપરવામાં આવે છે. આ પ્રકારે કમ્પ્યૂટરનો ઉપયોગ થતો હોય છે, ત્યારે પોતાના કમ્પ્યૂટરથી માઈનિંગ થઈ રહ્યું છે તે વાતથી કમ્પ્યૂટરની માલિકી ધરાવનાર વ્યકિત અજાણ હોય છે તેના દ્વારા પોતાના કમ્પ્યૂટરના રોજિંદા વપરાશમાં કમ્પ્યૂટર ધીમું કામ કરવા લાગે છે. કારણકે કમ્પ્યૂટરમાં સમાંતરે માઈનિંગ કામગીરી પણ ચાલતી હોય છે.

### લાગુ પડતી કલમો

આઈ.ટી. એક્ટ કલમ ૬૬, ૬૬(સી), ૬૬(ડી)

“મની લોન્ડરિંગ એક્ટ – ૨૦૦૨” અન્વયે લાગુ પડતી કલમો




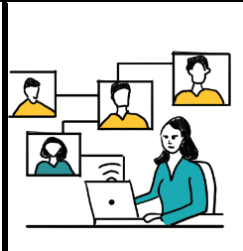



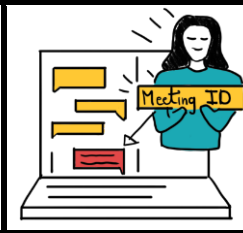

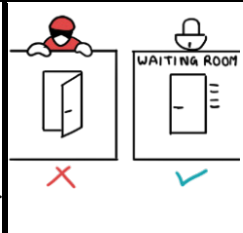
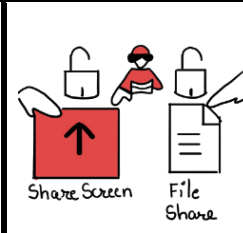
		
<p>રૂપા સોફ્ટવેર ડેવલપર હતી. તે ઘરેથી કામ કરતી હતી.</p>	<p>તે તેના કોડને એકિઝક્યુટ કરવા માટે બે ખૂબ પાવરફૂલ લેપટોપ્સનો ઉપયોગ કરતી.</p>	<p>ઘીમે ઘીમે તેને ખ્યાલ આવે છે કે, તેના કમ્પ્યુટરની ઝડપ સામાન્ય કરતાં ઘણી ઓછી થઈ ગઈ હતી.</p>
		
<p>આ ઉપરાંત, તેને લેપટોપ્સ પણ વારંવાર ચાર્જ કરવાની જરૂર પડતી હતી.</p>	<p>પ્રોસેસ મેનેજર ખોલ્યા બાદ, તેને ધ્યાને આવે છે કે, તેના લેપટોપ્સમાં કેટલીક અજાણી એપ્લિકેશન્સ ચાલી રહી હતી.</p>	<p>આ ક્રિપ્ટોજેકિંગ એપ્લિકેશન્સ હતી, જે બિટકોઇન્સ માઈન કરવા માટે તેના લેપટોપ્સનો ઉપયોગ કરતી હતી.</p>
		
<p>તેને એક અજાણી લિંક પર ક્લિક કર્યું હતું, જેના દ્વારા આ એપ્લિકેશન્સ ઈન્સ્ટોલ થયેલ હતી.</p>	<p>તેના લેપટોપ્સનો ઉપયોગ કરીને સાયબર ક્રિમીનલ, ક્રિપ્ટો માઈનિંગ કરી ઘણા પૈસા કમાયા હતા.</p>	<p>જો તેને સારું એન્ટિ વાઈરસ તથા ક્રિપ્ટો જેકિંગથી સુરક્ષિત રાખે તેવું બ્રાઉઝર એક્સ્ટેન્શન ઈન્સ્ટોલ કર્યું હોત, તો તે ક્રિપ્ટો જેકિંગથી બચી શકી હોત.</p>

### ૩૫. વીડિયો કોન્ફરન્સ

હાલની પરિસ્થિતિઓમાં ઓનલાઇન ક્લાસ, મિટિંગ કોન્ફરન્સ તથા અન્ય વિવિધ બાબતે અન્ય લોકો સાથે વીડિયો કોન્ફરન્સ મારફતે એકબીજાનો સંપર્ક કરવાનું ચલણ વધ્યું છે. ઉપયોગકર્તાઓ દ્વારા વીડિયો કોન્ફરન્સ યોજવાની સુવિધા પૂરી પાડનાર વિવિધ પ્લેટફોર્મ દ્વારા આપવામાં આવતી વિવિધ સિક્યોરિટી સેટિંગ્સ અવગણવામાં આવે છે, જેનો લાભ લઈને સાચબર કિમીનલ્સ દ્વારા ગેરરીતિ આચરવામાં આવે છે.

### લાગુ પડતી કલમો

આઈ.ટી. એક્ટ કલમ ૬૬, ૬૬ (સી), ૬૭, ૬૭ (એ)





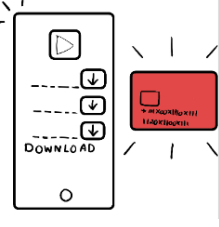
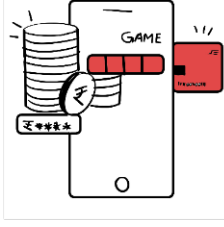

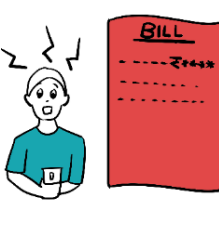
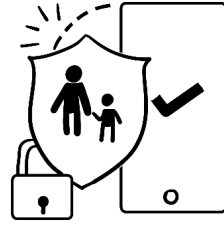
		
<p>અક્ષિતા એક મલ્ટિનેશનલ કંપનીમાં ટીમલીડર તરીકે નોકરી કરતી હતી. તાજેતરમાં તેણે ઘરેથી કામ કરવાનું પસંદ કર્યું હતું.</p>	<p>તે ઓફિસની કામગીરી માટે પોતાની ટીમના સભ્યો સાથે દરરોજ ઓનલાઇન મિટિંગ કરતી હતી.</p>	<p>ઘણી વખતે તેના ગ્રાહક (ક્લાયન્ટ) પણ કામગીરી વિશે જાણવા તથા જરૂરી સુધારા જણાવવા માટે ઓનલાઇન મિટિંગથી કરતા.</p>
		
<p>એક દિવસ સવારે, ક્લાયન્ટ મિટિંગ દરમિયાન, અજાણ્યા ચુક્રે (ઉપયોગકર્તાએ) લોગઇન કરીને બીભત્સ કિલપ પોસ્ટ કરી હતી.</p>	<p>આ શરમજનક ઘટનાથી અક્ષિતાએ તુરંત લોગ-ઓફ કરી દીધું હતું.</p>	<p>તેને આ મિટિંગનું આઈડી તથા પાસવર્ડનો મેસેજ મિટિંગના ડિસ્કશન ફોરમમાં પોસ્ટ કરીને ભૂલ કરી હતી.</p>
		
<p>કોઈ ક્લાયન્ટના (ગ્રાહકના) એક અસંતુષ્ટ કર્મચારીએ અલગ નામથી આ મિટિંગમાં લોગઇન કર્યું હતું.</p>	<p>આ મિટિંગ દરમિયાન ભાગ લેનારાઓને જોઈ શકાય તે માટે પ્રતીક્ષાખંડ (વેઈટિંગ રૂમ) ચાલુ ન હતો.</p>	<p>ભાગ લેનારાઓ માટે ફાઇલ શેર કરવાની તથા સ્ક્રીન શેર કરવાની મંજૂરી બંધ કરેલ ન હતી.</p>

### ૩૬. મોબાઈલ ફોન અને નાનાં બાળકો

આજકાલ માતાપિતા દ્વારા નાનપણથી જ બાળકોને મોબાઈલ ફોન વાપરવા માટે આપવામાં આવે છે. બાળક મોબાઈલના ઉપયોગથી ગેમ્સ, અશ્લીલ, ઘાતકી, શોષણ કરે તે પ્રકારના વિવિધ કન્ટેન્ટ અથવા માહિતીના સંપર્કમાં આવી શકે છે. જેનાથી બાળકોના મન પર દુષ્પ્રભાવ પડે છે અને બાળક અયોગ્ય/ગેરકાનૂની પ્રવૃત્તિ પણ કરી શકે છે. બાળકોને ફોન આપતા પેલા ફોનમાં “પેરેન્ટલ કંટ્રોલ” લાગુ કરી શકાય છે. બાળકોને મોબાઈલ ફોનની ઓછી ટેવ પડે તે મુજબ તેને બહાર ખુદ્ધા મેદાનમાં રમવા માટે તથા ઓનલાઈનના બદલે આસપાસના લોકો સાથે વાતચીત કરે તે માટે પ્રેરિત કરવા જોઈએ.

### લાગુ પડતી કલમો

આઈ.ટી. એક્ટ કલમ ૬૬ (સી)

		
<p>સુમન તેના નવ વર્ષના પુત્ર અર્ણવ સાથે એકલી રહેતી હતી.</p>	<p>તે તેના ઘરની નજીકના બ્યુટીપાર્લરમાં કામ કરતી હતી.</p>	<p>રોગચાળાની પરિસ્થિતિના કારણે બધા કલાસ ઓનલાઇન થઈ ગયા હતા જેથી અર્ણવ તેની માતાના મોબાઇલ ફોનથી ઓનલાઇન કલાસમાં હાજરી આપતો.</p>
		
<p>અર્ણવ કલાસ ચાલતા હોય ત્યારે કલાસમાં હાજરી આપવાના બદલે વીડિયો ગેમ રમતો હતો</p>	<p>તે તેની માતાના ક્રેડિટ કાર્ડના ઉપયોગથી પૈસા ચૂકવીને એપ્સ ડાઉનલોડ કરતો.</p>	<p>અમુક વાર તે વીડિયો ગેમમાં ઝડપથી જીતી જવા માટે પણ પૈસા ચૂકવતો.</p>
		
<p>અર્ણવ નાણાં ચુકવણીના મેસેજ કિલિટ કરી નાખતો જેથી તેની માતાને આ બાબતની ખબર પડતી નહીં.</p>	<p>સુમનને તેના ક્રેડિટ કાર્ડમાંથી રૂ. ૧૪,૦૦૦ પ્લેસ્ટોરમાં ચૂકવવાયા હોવાનો ખ્યાલ આવતા તેને આઘાત લાગ્યો હતો.</p>	<p>જો તેને ફોનમાં પેરેન્ટલ કંટ્રોલ ચાલુ રાખ્યું હોત, તો અર્ણવ ખાલી શિક્ષણ માટે જ તેના મોબાઇલ ફોનનો ઉપયોગ કરી શક્યો હોત.</p>






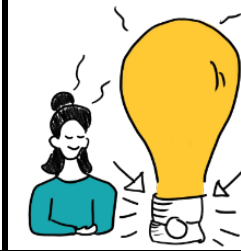



### ૩૭. સ્માર્ટ હોમ્સ

સ્માર્ટ હોમ્સ ડિવાઈસિસમાં (ઉપકરણોમાં) આપના જન્મ તારીખ, આપના બેન્ક એકાઉન્ટ્સથી લઈને અન્ય ઘણીખરી અંગત/ નાણાંકીય માહિતીનો સંગ્રહ કરવામાં આવેલ હોય છે. જો આવાં ઉપકરણો તથા તેમાં રાખવામાં આવેલ માહિતી યોગ્ય રીતે સુરક્ષિત કરવામાં આવેલ ન હોય, તો હેકર્સ તેને હેક કરીને આપની માહિતી ચોરી શકે છે અને તેને ગેરકાનૂની કામમાં વાપરી શકે છે.

#### લાગુ પડતી કલમો

ઇ.પી.કો. કલમ ૩૫૪, ૩૫૪(સી), ૫૦૯

આઈ.ટી. એક્ટ કલમ ૬૬, ૬૬(ઇ)

		
<p>સાક્રિયા એક ટેકનોલોજીની જાણકાર ગૃહિણી હતી. તેને નવાં-નવાં ગેઝેટ્સ ખરીદવા અને વાપરવા ગમતાં હતાં.</p>	<p>એકવાર તે એક ગુજરી બજારની મુલાકાતે ગયેલ. જ્યાંથી તેણે સસ્તા ભાવે ઈન્ટરનેટ ઓફ થિંગ્સ (IOT) ઉપકરણની ખરીદી કરી હતી.</p>	<p>તે ઉપકરણ ૬૦% સુધીની ડિસ્કાઉન્ટેડ કિંમત પર મેળવીને સાક્રિયા ખૂબ ખુશ થઈ ગઈ હતી.</p>
		
<p>સાક્રિયાએ ત્યાંથી ખરીદેલ સ્માર્ટ બલ્બ પોતાના બેડરૂમમાં લગાવેલ હતો.</p>	<p>આ બલ્બ તેના મોબાઇલ ફોનથી નિયંત્રણ કરી શકાતો, તેનો કલર બદલી શકાતો તથા બંધ/ચાલુ કરી શકાતો હતો.</p>	<p>તે જાણતી ન હતી કે, વાઈફાઈ સાથે કનેક્ટેડ રહેતા આ બલ્બમાં છૂપીરીતે નેનો કેમેરા લગાવેલ હતો.</p>
		
<p>આ કેમેરા તેના બેડરૂમની બધી જ પ્રવૃત્તિઓ રેકોર્ડ કરી શકતો અને તેને પોતાના સર્વર પર અપલોડ કરી શકતો.</p>	<p>તે જાણતી ન હતી કે, આ IOT ઉપકરણ અધિકૃત વેચાણકર્તા પાસેથી જ ખરીદવા જોઈએ અને જરૂરી સુરક્ષા સેટિંગ્સ કરેલા હોવા જોઈએ.</p>	<p>ઈન્ટરનેટથી જોડાયેલ કોઈ પણ ઉપકરણ જાસૂસી કરવા માટે ઉપયોગમાં લઈ શકાય છે. ટેકનોલોજી બેઢારી તલવાર છે.</p>

### ૩૮. માઈક્રો લોન્સ





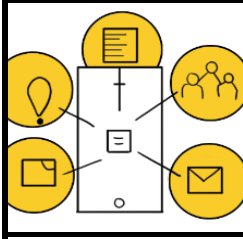


માઈક્રો લેન્ડિંગ સેવા પૂરી પાડતી અપ્સથી કામગીરી કરતી, ઘણીખરી (ગેરકાનૂની) કંપનીઓ છે, જે ખૂબ જ સરળતાથી લોન્સ આપે છે. આવી કંપનીઓ યુવાન/કિશોર વયના લોકોને લોન્સ આપે છે, જેઓ સામાન્ય રીતે લોન્સ અને તેની પદ્ધતિથી માહિતગાર હોતા નથી. સેવાનો લાભ લેનાર લોકો પાસેથી ત્યારબાદ ઉચ્ચ વ્યાજદર કે વિવિધ ફીસના નામે નાણાં વસૂલવામાં આવે છે અને જો તેઓ નાણાં ચૂકવવા સક્ષમ ન હોય તો તેઓને વિવિધ રીતે પરેશાન કરવામાં આવે છે.

### લાગુ પડતી કલમો

ઈ.પી.કો. કલમ ૩૪, ૧૨૦(બી), ૩૮૪, ૪૨૦, ૪૯૯,  
૫૦૦, ૫૦૩, ૫૦૬, ૫૦૭

રિઝર્વ બેન્ક ઓફ ઈન્ડિયા અધિનિયમ ૧૯૩૪ અન્વયે લાગુ  
પડતી વિવિધ કલમો



		
<p>સમંથા એલિજનિયરિંગના છેલ્લા વર્ષમાં અભ્યાસ કરતી હતી અને તેની કોલેજની નજીક હોસ્ટેલમાં રહેતી હતી.</p>	<p>તેનાં માતાપિતા દર મહિને તેના ખર્ચ માટે રૂ. ૫૦૦૦ મોકલતાં હતાં.</p>	<p>સમંથા પાસે વધારાની કોઈ આવડત ના હોઈ તેને કેમ્પસ પ્લેસમેન્ટથી નોકરી મળતી નથી.</p>
		
<p>તેને ઓનલાઇન કલાસમાં એડમિશન માટે રૂ. ૧૦,૦૦૦ની જરૂર હતી. તે તેનાં માતાપિતાની આર્થિક પરિસ્થિતિ ખરાબ હોવાથી તેમના પાસે પૈસા માગતાં ખચકાતી હતી.</p>	<p>એક દિવસ તેણે તેના કમ્પ્યુટરમાં એક જાહેરાત જોઈ, જેમાં રૂ. ૧૦૦૦૦ની લોન કોઈ પણ ડોક્યુમેન્ટ વગર મળતી હતી, જેનાથી ખુશ થઈ તેણે જણાવ્યા મુજબ એપ ઇન્સ્ટોલ કરી હતી.</p>	<p>તેને ઓનલાઇન કલાસથી કોર્સ પૂર્ણ કર્યો હતો. તેમ છતાં તે નોકરી મેળવી શકતી નથી. જેથી તે લોન ભરવા સક્ષમ ન હતી.</p>
		
<p>તે જાણતી ન હતી કે આ એપ તેના કોન્ટેક્ટ લિસ્ટ, લોકેશન તથા તેના ફોનમાં રહેલ અન્ય ડેટાને એક્સેસ કરી શકતી હતી.</p>	<p>તે જે એપ થકી લોન લે છે તે કંપનીના લોકો તેને ડરાવવા, ધમકાવવા લાગ્યા હતા. તેઓ તેના મિત્રોને પણ ધમકી આપવા લાગ્યા હતા.</p>	<p>ઘણી શાર્ક લોન એપ્લિકેશન્સ રકમ વસૂલવા માટે ગુંડાઓ પણ મોકલે છે અને મેળવેલ લોન પર ભારે વ્યાજ પણ વસૂલ કરે છે.</p>


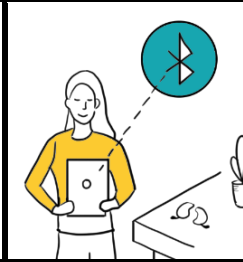
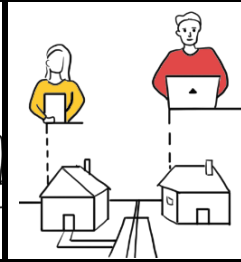


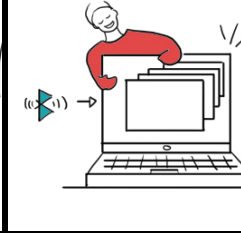
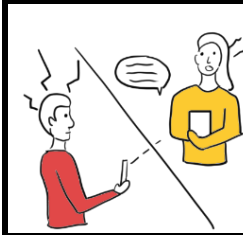

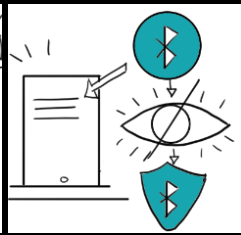
### ૩૯. બ્લૂ સ્નાર્ફિંગ

બ્લૂ સ્નાર્ફિંગ એક પ્રકારની હેકિંગ કરવાની પદ્ધતી છે જેમાં હેકર્સ, ઉપયોગકર્તા દ્વારા બેદરકારીથી તેઓના ઉપકરણનું બ્લૂટૂથ જ્યારે ડિસ્કવરેબલ મોડમાં ચાલુ રાખી મૂકવામાં આવે છે, તેનો લાભ લઈને ઉપયોગકર્તાને જાણ ન થાય તે રીતે તેના ઉપકરણ સાથે કનેક્ટ થઈ જાય છે, જેનાથી તે ઉપયોગકર્તાની અંગત માહિતી ચોરી કરી શકે છે અને તેનો ગેરકાનૂની પ્રવૃત્તિમાં ઉપયોગ કરી શકે છે.

### લાગુ પડતી કલમો

આઈ.ટી. એક્ટ કલમ ૬૬, ૬૬ (સી), ૬૬ (ડી)

ઈ.પી.કો. કલમ ૪૧૯, ૪૨૦

		
<p>આલિયાએ ઓનલાઇન અભ્યાસ કરી શકાય તે માટે ગુજરી બજારમાંથી એક સરતા ટેબલેટની ખરીદી કરી હતી.</p>	<p>તે હંમેશાં તેનાં ટેબલેટનું બ્લૂટૂથ ચાલુ રાખતી, જેથી તેનાં હેડફોન ટેબલેટ સાથે જોડાયેલા રહેતા.</p>	<p>તેનો પાડોશી અનુશ, ડાર્ક વેબથી હેકિંગના કોર્સની મદદથી હેકિંગ શીખ્યો હતો.</p>
		
<p>નબળી સિક્યોરિટી ધરાવતાં કોઈ પણ ડિજિટલ ડિવાઇઝ સાથે કનેક્ટ કરી શકે તે મુજબના સોફ્ટવેર અનુશે ડાઉનલોડ કર્યા હતા.</p>	<p>બ્લૂટૂથની રેન્જ ૧૦ મીટરની હોવાથી આલિયાના ટેબ સાથે કનેક્ટ કરવા માટે એક દિવસ અનુશ આલિયાના બગીચામાં છુપાઈ ગયો.</p>	<p>અનુશ હવે આલિયા ના ટેબ સાથે કનેક્ટ થઈ ગયો હતો, તે ટેબલેટમાંથી તમામ ફાઇલ્સ/ફોલ્ડર્સ જોઈ શકતો હતો અને ટેબલેટનો IMEI નંબર પણ તેના પાસે આવી ગયો હતો.</p>
		
<p>અનુશે તેના ટેબલેટ પરના તમામ મેસેજ અને કોલ્સ પોતાના નંબર પર ફોરવર્ડ કરી લીધા.</p>	<p>આલિયાને તેના ટેબમાંથી ઘણા ફોટો અને ફાઇલ્સ ન હોવાનું ધ્યાને આવેલ; તેને ફોન પણ આવતા બંધ થઈ ગયા હોવાનો અહેસાસ થયો.</p>	<p>જો આલિયાએ પોતાના બ્લૂટૂથનાં MAC આઈ.ડી. ને છૂપો રાખેલ હોત તો આ ઘટના થતી નહીં અને તે સુરક્ષિત રહેતી.</p>

## ૪૦. ખોવાયેલો મોબાઈલ ફોન

આપણે આપણા મોબાઈલ ફોનમાં દરેક અંગત/નાણાંકીય માહિતી રાખીએ છીએ. આપણા ફોનમાં રહેલ ઘણી માહિતી ભાવનાત્મક રીતે આપણા માટે અમૂલ્ય હોય છે. આપણો આ ફોન જ્યારે ચોરાઈ જાય છે અથવા તો આપણાથી જ ખોવાઈ જાય છે ત્યારે શક્યતઃ તે ખરાબ ઈરાદા ધરાવનાર વ્યક્તિના હાથમાં જાય છે. આ પ્રકારે ફોન ગુમાવવાના કારણે આપણે ઘણી માહિતી ગુમાવીએ છીએ ઉપરાંત આપણો ફોન અયોગ્ય વ્યક્તિના હાથમાં જાય છે ત્યારે તે ફોનમાં રહેલ માહિતીનો ઉપયોગ ગેરકાનૂની પ્રવૃત્તિમાં કરી શકે છે.

### લાગુ પડતી કલમો

ઈ.પી.કો. કલમ ૩૭૯

આઈ.ટી. એક્ટ કલમ ૬૬, ૬૬ (બી)

		
<p>અનામિકાને મોબાઈલ ઉપયોગ કરવાની ખૂબ ટેવ હતી. તે સ્નેપચેટ, વ્હોટ્સેપ અને ઈન્સ્ટાગ્રામનો નિયમિત ઉપયોગ કરતી હતી</p>	<p>અનામિકા તેની મિત્ર દિવ્યા સાથે એક વખત મેળામાં ગઈ હતી.</p>	<p>અનામિકા અને દિવ્યા એક ચકડોળને જોઈને ઉત્સાહથી ટિકિટ ખરીદીને ચકડોળમાં બેઠાં.</p>
		
<p>તેના ધ્યાન બહાર તેનો ફોન ખિસ્સામાંથી પડી ગયો હતો.</p>	<p>ચકડોળ જ્યારે ઉપર તરફ ગયું ત્યારે તે સેલ્ફી લેવા માટે મોબાઈલ ફોન કાઢવા ખિસ્સા તપાસતી હતી.</p>	<p>મોબાઈલ ફોન ખોવાયો હોવાની જાણ થતાં તેણે તુરંત દિવ્યાના ફોનથી પોતાના ફોન ઉપર કોલ કર્યો.</p>
		
<p>મોબાઈલ ફોન મેળવનાર વ્યક્તિએ તુરંત કોલ કાપી નાખ્યો અને ફોન સ્વિચ ઓફ કરીને પોતાના ખિસ્સામાં મૂકી દીધો.</p>	<p>અનામિકા “ફાઈન્ડ માય ડિવાઈઝ” ફિચરનો ઉપયોગ કરીને પોતાનો ફોન શોધી શકી હતો.</p>	<p>તે દૂરથી ફોન અડક્યા વગર પોતાનો ફોન પણ ફોરમેટ કરી શકી હતો.</p>

## યાદ રાખો

સાયબર ગુનેગાર આપના સાથે છેતરપિંડી કરવાના ઈરાદાથી આપને ગમે તેવી લાલચ આપે, ડરાવે, ઉતાવળ કરવા મજબૂર કરે તેવી પરિસ્થિતિ ઊભી કરે, પરંતુ આપે આ બાબતે સમજપૂર્વક, મક્કમપણે, ખૂબજ ધીરજથી પરિસ્થિતિનો સામનો કરવાનો છે.



આપના સાથે થયેલ સાયબર ક્રાઈમની ફરિયાદ કરવા માટે ડાયલ ૧૦૦ અને નવનિર્મિત ૭ જિલ્લાઓ માટે ડાયલ ૧૦૦/૧૧૨ થકી પોલીસ વિભાગનો સંપર્ક કરો.

સાયબર ક્રાઈમ જાગૃકતા કેળવવા તથા સાયબર ક્રાઈમ વ્રાન્ય, અમદાવાદ શહેરના આ અભિયાનમાં જોડાવવા માટે [www.cybersafeahmedabad.org](http://www.cybersafeahmedabad.org) website તથા સોશિયલ મીડિયા પ્લેટફોર્મનો ઉપયોગ કરશો.

 @ahmedabadpolice  @ahmedabadpolice

 @AhmedabadPolice  Cyber Crime Branch, Ahmedabad City

સંપર્ક:-

સાયબર ક્રાઈમ વ્રાન્ય, અમદાવાદ શહેર  
બંગલા નંબર - ૧૫, ડફનાળા,  
શાહીબાગ, અમદાવાદ- ૩૮૦ ૦૦૪