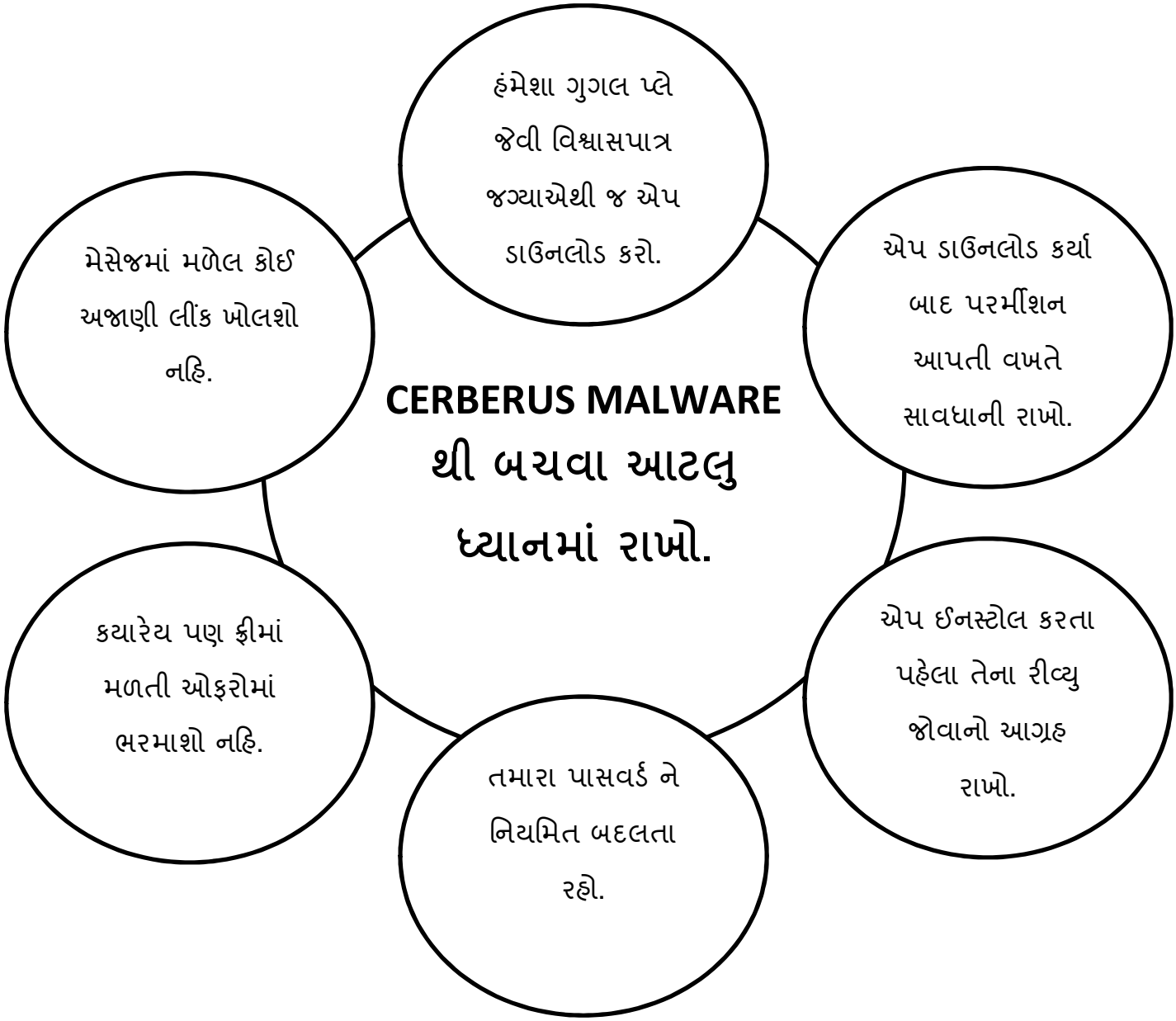
# ખતરનાક બેન્કીંગ વાયરસ CERBERUS થી સાવધાન

**આ વાયરસ તમારા ફોનમાં મેસેજમાં આવતી અજાણી લીંક પર કલીક કરવાથી અથવા અનઓથોરાઈઝડ એપ ડાઉનલોડ કરવાથી આવે છે.**



# સાયબર અવેરનેશ થી આપની સલામતીઃ

પ્રિય ગ્રાહકમિત્રો,

આપનાં નાણાંની સલામતી, એ અમારી નૈતિક ફરજ છે. આજકાલ અવનવી રીતે લોકો સાયબર ક્રાઈમનો ભોગ બની રહયા છે. જે અંગે જાગૃતિ ફેલાવવાનાં ભાગરૂપે, બેન્ક આ એક નાની પુસ્તિકા આપ સમક્ષ પ્રસ્તુત કરે છે. જેનો અભ્યાસ કરી, અમલ કરશો તો, આપ સાઈબર ક્રાઈમનો ભોગ બનતા બચી શકો છો.

આજકાલ ઓનલાઈન શોપીંગ, ઓનલાઈન બેન્કીંગ વગેરે, રોજીંદી જીંદગીનો એક ભાગ થઈ ગયો છે પરંતુ એની સાથે સાથે સાયબર ફ્રોડ પણ દિન પ્રતિદિન વધતાં જાય છે. જરા પણ ગફલત સાયબર ફ્રોડનો ભોગ બનાવી શકે છે.

આ પુસ્તિકામાં આપેલ માહિતી, ખાસ કરીને કુકરવાડા નાગરિક સહકારી બેન્કનાં ગ્રાહકો માટે જ હોઈ, ઈન્ટરનેટ બેન્કીંગથી થતી છેતરપીંડીનો સમાવેશ કરેલ નથી.

**ધી કુકરવાડા નાગરિક સહકારી બેંક લિ.**
**જનરલ મેનેજર / સી.ઈ.ઓ**

**(૧) OTP કોઈને પણ આપવો નહીં:**

ઓન લાઈન ખરીદી કરતી વખતે કે પેમેન્ટ કરતી વખતે અને હવે તો, ATM માંથી નાણાં ઉપાડતી વખતે પણ, આપને OTP ની જરૂર પડે છે. પરંતુ તમારા મોબાઈલમાં આવેલ OTP નંબર મેળવવા માટે આજકાલ, છેતરપીંડી કરવાવાળા માણસો, "હું બેન્કમાંથી બોલું છું." અથવા "હું ડેબીટ કાર્ડ વિભાગમાંથી બોલું છું", "સાયબર ક્રાઈમમાંથી બોલું છું" વિગેરે કીમીયાઓ અપનાવી તમારી પાસેથી ચેનકેન પ્રકારે OTP નંબર મેળવવા પ્રયત્ન કરે છે. ઉપરાંત આવી વ્યકિતઓનાં મોબાઈલનાં True Caller માં પણ જે તે વિભાગનાં નામ લખેલ હોઈ, આપ OTP નંબર આપવાની ભૂલ કરી બેસો છો. માટે આ રીતે વિશ્વાસમાં આવી OTP નંબર કોઈને પણ આપવો નહીં.

**(૨) આપનો PIN, CVV તેમજ પાસવર્ડ:**

OTP ની જેમ જ આપનાં ડેબીટ કાર્ડનાં પાછળનાં ભાગ પર છાપેલ CVV તેમજ કાર્ડનાં ઉપયોગ માટે આપે નકકી કરેલ PIN તેમજ પાસવર્ડ તો OTP કરતાં પણ વધુ અગત્યતા ધરાવે છે. જે અંગે નીચેનાં મુદ્દાઓ ધ્યાનમાં રાખશો તો સાઈબર ફ્રોડથી આપ બચી શકો છો.

- આપનાં મોબાઈલ ફોનમાં ATM કાર્ડનાં આગળ-પાછળનો ફોટો પાડીને સેવ રાખવો નહીં.
- આપનાં કાર્ડના PIN તેમજ CVV નંબર કયારેય કોઈને આપવા નહીં.
- કોઈપણ પાસવર્ડ, PIN કેCVV યાદ રાખવા માટે મોબાઈલ ફોનની ફોનબુકમાં કે કોઈ કાગળ લખી રાખવા નહીં.
- આપનો ડેબિટ કાર્ડ અપડેટ કરવાનો હોવાથી હાલ, બ્લોક કરેલ છે એવા બહાને આપને ફોન કરીને આપનાં કાર્ડનો PIN,CVV કે પાસવર્ડ માંગવામાં આવે છે, તો આવા પ્રકારના ફોનથી સાવચેત રહેવું અને આપણી બેન્ક શાખામાં ફોન કરી, કાર્ડ બ્લોક થયો છે કે નહીં તે જાણી લેવું.
- આ ઉપરાંત કેવાયસી(KYC) રીન્યુ કે અપડેટ કરવાનાં બહાનાં હેઠળ ફોન કે મેસેજ કરી, આપની પાસે PIN, CVV કે પાસવર્ડ માંગવામાં આવે છે તો, આવા પ્રસંગે પણ, આપે આપની બેન્ક શાખાનો સંપર્ક કરી સાચી હકીકત જાણવી જરૂરી છે.

**(3) આજકાલ ચાલી રહી છે નવી Fraud....કરવાની રીતઃ**

તમને કોઈ બહેનનો ફોન આવશે કે ભૂલથી તમારા ખાતામાં ૧૦૦ રૂપિયા ટ્રાન્સફર થઈ ગયા છે. તમે ચેક કરશો તો સાચેસાચ રૂપિયા આવ્યા હશે. પછી તે કહેશે કે પૈસા પાછા કરવા જે *OTP* આવ્યો છે તે મને મોકલો. આ trap નો ભોગ બનતા નહીં. *OTP* મોકલતાં નહીં. પરંતુ સામેવાળાને જો *OTP* આપશો તો ફસાઈ જશો.

બીજી પણ એક રીત અપનાવીને ફોન આવે છે કે, "મારી નોકરીના અરજીના ફોર્મમાં ભૂલથી તમારો નંબર લખાઈ ગયો છે. નંબર મળતા આવતા હોવાથી આ ભૂલ થઈ છે. નંબર ચેન્જ કરવા માટે મારી કંપનીએ તમને *OTP* મોકલ્યો હશે. તો Please એ મને આપો ને..

(આ ફોન એટલો આજીજીભર્યો હોય છે કે તેમાં ફસાઈ જવાય).
યાદ રાખશો...કોઈપણ ભોગે કયારેય કોઈને *OTP* શેર ના કરશો.
માટે હાલમાં લોકો ગુગલ ઉપર સર્ચ કરી હેલ્પલાઈન નંબર અથવા કસ્ટમર કેર નંબર શોધતા હોય છે અને ફ્રોડલોકો ધ્વારા પ્રતિષ્ઠિત કંપનીના હેલ્પલાઈન નંબરમાં પોતાના નંબર નાંખી તમને મદદ કરવા માટે લીન્ક મોકલાવી અથવા ગીફ્ટ વાઉચરના મેસેજ મોકલી તેઓ તરફથી **Quick Support/Any Desk** નામની એપ્લીકેશન ડાઉનલોડ કરાવી મોબાઈલ ફોન રીમોટ કરી ઓનલાઈન નાણાંકીય વ્યવહારની બધી વિગતો જાણી લોકોના એકાઉન્ટમાંથી નાણાંની છેતરપીંડી કરતા હોય છે. આવી તમામ લીન્કોથી સાવધાન રહેવું જોઈએ અને કોઈ અજાણ્યા વ્યકિતઓ ફોનમાં આપની પાસે કોઈપણ પ્રકારની પ્રોસેસ કરાવે તો તેમ નહીં કરવુ અને મોબાઈલમાં આવતો કોઈપણ પ્રકારનો ઓટીપી કોઈને પણ આપવો જોઈએ નહીં.

### (૫) સોશિયલ મીડીયાઃ

સોશિયલ મીડીયા વોટ્સએપ ફેસબુક જેવી એપ્લીકેશનો ઉપર ફ્રોડ લોકો ધ્વારા 'કોન બનેગા કરોડપતિ' ના નામે ખોટી જાહેરાત મોકલી તેમજ લકી ડ્રો ના નામે મોટી રકમ મેળવવાની લાલચ આપી તેમજ બેંક એકાઉન્ટ વેરીફીકેશન કરવાના બહાને આમ જનતાને વિશ્વાસમાં લઈ મોટી રકમ મેળવવાના નામે બેંક ફી ભરવાના બહાને અથવા તો એક લીંક શેર કરી, ટ્રાન્ઝેકશન કરવા પ્રેરીત કરી ફ્રોડ કરે છે. જેથી આપે આ બાબતે સાવચેત અને સજાગ રહેવું જોઈએ.

સોશિયલ મીડીયા ફેસબુક OLX જેવી સાઈટ ઉપર આર્મી જવાનના નામનું ખોટુ/ફેક એકાઉન્ટ બનાવી તેમાં બાઈક, કેમેરા, ફર્નિચર, ગાડી જેવા સાધનો વેચાણ મુકી વેચાણના બહાને લોકોને વિશ્વાસમાં લઈ ખોટી સ્કીમો આપી પૈસા પડાવી ફ્રોડ કરવામાં આવે છે.

### (૬) પાસવર્ડ પોલીસી

- પોતાનો પાસવર્ડ મજબૂત હોવો જોઈએ અને સુરક્ષા ધોરણનું પાલન કરવું આવશ્યક છે.
- સમયાંતરે પાસવર્ડ બદલતું રહેવું જોઈએ અને પાસવર્ડ કયારેય કોઈ નોટબુકમાં લખવો નહીં કે મોબાઈલમાં સેવ કરવો નહીં.
- પાસવર્ડ રાખતી વખતે બિન અલ્ફાબેટીક અક્ષરો જેવા કે *, **@, #** વગેરે અવશ્ય રાખવા જોઈએ.
- આપનું નામ, જન્મ તારીખ, વ્હીકલ નંબર કે ઘર નંબરને, પાસવર્ડ તરીકે પસંદ કરશો નહીં. હેકર્સ, આવા પ્રકારનાં પાસવર્ડને હેક કરી શકે છે જેને ધ્યાનમાં રાખી યોગ્ય કેરેક્ટર્સ,અલ્ફા, બિન અલ્ફા,ડીજીટ વગેરેનો ઉપયોગ કરી મિક્સ પાસવર્ડ રાખવો આપના હિતમાં છે.

### (૭) બેદરકારી ભારી પડી શકે છેઃ

ઓરીએન્ટલ બેન્ક ઓફ કોમર્સનાં એક ગ્રાહકનાં કિસ્સામાં એવું બન્યું હતું કે, તે ગ્રાહકનાં ખાતામાંથી કોઈક ત્રાહિત વ્યકિતએ એટીએમ પરથી રોકડ ઉપાડયા હતાં. તે ગ્રાહકે, બેન્કને ફરીયાદ કરી સદર ફ્રોડ અંગે બેન્કને જાણ કરી હતી. પરંતુ બેન્કે સદર ખોટી રીતે થયેલ ઉપાડની રકમ જમા ન

આપતાં, સદર કિસ્સો, જિલ્લા ગ્રાહક અદાલત અને ત્યાંથી રાજય કમીશન થઈ છેવટે નેશનલ કમિશન સુધી પહોંચ્યો હતો. નેશનલ કમિશને ચુકાદામાં જણાવ્યું હતું કે ફરીયાદી બેન્કની સેવામાં ક્ષતિ હોવાનું દર્શાવી શકયા ન હતાં અને ત્રાહિત વ્યકિત કે જેણે ખોટી રીતે નાણાંનો ઉપાડ કરેલ હતો એની સામ FIR નોંધાવી ન હતી કે તે ત્રાહિત વ્યકિતને કાનુની કાર્યવાહીમાં પક્ષકાર પણ બનાવી ન હતી. જેથી ફરિયાદ રદ કરતો હુકમ નેશનલ કમિશન ધ્વારા કરવામાં આવેલ હતો.

બીજા એક સ્ટેટ બેંકનાં કિસ્સામાં, પત્નીનો એટીએમ કાર્ડ, પતિ ધ્વારા એટીએમમાંથી રોકડ ઉપાડવા ઉપયોગ કરવામાં આવ્યો હતો પરંતુ સદર ખાતેદારનું ખાતું ડેબિટ થઈ ગયું હતું પરંતુ, નાણાં મળ્યાં ન હતાં. આથી પત્નીએ ફરિયાદ કરવા છતાં સ્ટેટ બેન્કે નાણાં પરત આપ્યા નહોતાં. કોર્ટમાં કેસ ચાલતાં સ્ટેટ બેન્કે જણાવ્યું કે, સીસીટીવી કેમરો ચેક કરતાં, જણાવ્યું કે કાર્ડ જેનાં નામનો હતો તેનાં ધ્વારા, નાણાં ઉપાડવા ઉપયોગ થયો નહોતો અને કાર્ડ Non Transferable હોવાથી, સદર રકમ પરત કરવા બેન્ક જવાબદાર બનતી નથી. કોર્ટે, સ્ટેટ બેન્કની આ દલીલ માન્ય રાખી હતી.

**(૮) ATM કાર્ડ ખોવાઈ કે ચોરાઈ જાય તો:**

- જો આપનું ATM કાર્ડ ખોવાઈ જાય તો તુરંત જ આપની **બેંક શાખામાં અથવા તો C-Edge ટોલ-ફ્રી નં. ૧૮૦૦-૩૦૦૦-૦૬૨૦** પર તાત્કાલીક સંપર્ક કરી કાર્ડ બ્લોક કરો.
- આ ઉપરાંત **"The Kukarwada Nagarik Sahakari Bank Ltd" ની એપ ગુગલ એપ પરથી** ડાઉનલોડ કરી, આપ જાતે જ પોતાના ATM કાર્ડને બ્લોક કરી શકો છો.
- આ ઉપરાંત બેન્કની **વેબ સાઈટ "http://complaint.kukarwadabank.com/" પરથી Complaint બૂક કરાવી** જાણ કરી શકો છો.

**(૯) જો આપ કોઈપણ પ્રકારનાં સાયબર ક્રાઈમનાં ભોગ બનો તો?**

જો આપ સાયબર ક્રાઈમનાં ભોગ બનો તો, તુરંત

- તાત્કાલિક ઉપાય માટે, આપે **હેલ્પ લાઈન નંબર ૧૯૩૦ ઉપર સંપર્ક** કરી ફરિયાદ કરવી.
- સાયબર ક્રાઈમ સંબંધિત મદદ અને સલાહ માટે આપ સાઈબર ક્રાઈમ સેલ હેલ્પ લાઈન નં. ૦૭૯-૨૩૨૫૦૭૯૮ અને ઈમેઈલ "helpline-cyber-cid@gujarat.gov.in" અને "cc-cid@gujarat.gov.in" પર સંપર્ક કરી શકો છો.
- "CYBERVOLUNTEER.MHA.GOV.IN" ઉપર પણ ઓનલાઈન ફરિયાદ કરી શકાય છે અને ત્યારબાદ તેના પર થયેલ કાર્યવાહીનો આપ અહેવાલ મેળવી શકો છો.

**નોંધ – હેલ્પલાઈન નંબર પર ઘટનાની જાણ થાય તો ફરિયાદીએ નીચેની માહિતી આપવી પડશે.**

- ફરિયાદીનો મોબાઈલ નંબર
- બેંક/વોલેટ/વેપારીનું નામ જેમાંથી રકમ ડેબિટ કરવામાં આવી છે
- રકમ નંબર/વોલેટ આઈડી/મર્ચન્ટ આઈડી/યુપીઆઈ આઈડી/ જેમાંથી રકમ ડેબિટ કરવામાં આવી છે
- ટ્રાન્ઝેક્શન આઈડી અને તારીખ
- ડેબિટ કાર્ડ/ક્રેડિટ કાર્ડના ઓળખપત્રનો ઉપયોગ કરીને કરવામાં આવેલી છેતરપિંડીના કિસ્સામાં ડેબિટ કાર્ડ/ક્રેડિટ કાર્ડ નંબર
- વ્યવહારનો સ્ક્રીન શોટ અથવા છેતરપિંડી સંબંધિત અન્ય કોઈપણ માહિતી, જો ઉપલબ્ધ હોય તો

**(૧૦) સ્ક્રીન શેરીંગઃ**

છેતરપીંડી કરનારા, કંપની પોલીસી મુજબ **Quicksupport/Teamviewer/Any Desk** વગેરે જેવી એપ્સનો સ્ક્રીન શેર કરી, તેમાં જરૂરી વિગતો ભરાવી, તમારી બેન્કીંગ વિગતો જેવી કે **OTP/ MPIN/ User Name/ Password** વગેરે મેળવીને તમને ખબર પડે એ પહેલા તો તમારું બેલેન્સ ખાલી કરી નાખે છે. માટે, સ્ક્રીન શેરીંગ એપ કદી પણ ઈન્સ્ટોલ કરવી નહીં. બેન્ક કે અન્ય કોઈપણ સંસ્થા આ રીતની માહિતી કદી માંગતા નથી.

**(૧૧) સીમકાર્ડ સ્વેપીંગઃ**

ટેલીકોમ સર્વિસ પ્રોવાઈડરનાં કર્મચારીની મદદથી, છેતરપીંડી કરનાર, તમારા નંબર પર જારી કરેલ નવો સીમકાર્ડ મેળવી લે છે અને ત્યારબાદ ટેલીકોમ કંપની ધ્વારા ૪જી સીમકાર્ડ અપગ્રેડ કરવા માટે આપનો હાલનો સીમકાર્ડ બ્લોક કરવામાં આવે છે, એ પ્રકારનો ફોન કરવામાં આવે છે અને ત્યારબાદ તે સિમ નંબર તમને આપે છે. જે તમને SMS ધ્વારા કસ્ટમર કેર નંબર પર મોકલવાનું કહેવામાં આવે છે. જે એસએમએસ મળવાથી, કંપની આપનો જુનો સીમ બ્લોક કરીને નવો સીમ ચાલુ કરે છે, જે ખરેખર છેતરપીંડી કરનાર પાસે હોય છે અને આમ તે તમારાં બેન્કનાં નાણાંકીય વ્યવહાર માટેની તમામ ગુપ્ત માહિતી એની પાસે પહોંચી જતા, તે આપનું બેલેન્સ ખાલી કરી નાખે છે.

**(૧૨) ATM/ડેબીટ કાર્ડ કલોનીંગ**

છેતરપીંડી કરનાર, ATM મશીનમાં Card Slotમાં Scimmer મશીન ફીટ કરે છે. જેથી કેશ ઉપાડતી વખતે એટીએમ માં કાર્ડ દાખલ કરતાં જ, Scimmer મશીન આપનાં કાર્ડની મેગ્નેટીક સ્ટ્રીપને વાંચીને, તમારા કાર્ડનાં તમામ ડેટા એકત્ર કરે છે, ત્યારબાદ આ એકત્ર કરેલ ડેટાને નવા કોરા કાર્ડ પર Rewrite કરે છે અને આ રીતે કલોન કરેલ કાર્ડનો ઉપયોગ કરી અન્ય એટીએમ માંથી નાણાંનો ઉપાડ કરી લે છે.

આ પ્રકારની છેતરપીંડીથી બચવું હોય તો

(૧) તમારો PIN અવારનવાર બદલતા રહો.

(૨) ATM માંથી નાણાં ઉપાડતી વખતે, ATM મશીનમાં કોઈ વધારાનું ડીવાઈસ લાગેલ નથી તે ચેક કરો.

(3) બને ત્યાં સુધી જે ATM નો ઉપયોગ વધુમાં વધુ થતો હોય તેવા ATM માંથી નાણાં ઉપાડવાનું પસંદ કરો.

**(૧૩) Juice Jacking:**

આ પ્રકારની છેતરપીંડીમાં જાહેરમાં ચાર્જીંગ માટે મુકવામાં આવેલ USB Port નો ઉપયોગ થાય છે. છેતરપીંડી કરનારા એ જ USB Port નો ઉપયોગ, તમે ચાર્જ કરવા મુકેલ મોબાઈલ, ટેબલેટ કે લેપટોપનાં ડેટા ચોરવા માટે કરે છે.

આ પ્રકારની છેતરપીંડીથી બચવા, જાહેરમાં મુકવામાં આવેલ USB Port માં ચાર્જ કરતાં પહેલા (૧) તમારા ફોનમાં "Data Transfer" ને Disable કરો. (૨) તમારા મોબાઈલને સ્વીચ ઑફ કરી દો. (૩) શકય હોય તો પાવર બેન્ક સાથે રાખો અને હવે તો બજારમાં "**Data Disabled charging cable**" પણ મળે છે.