ધી સધર્ન ગુજરાત ચેમ્બર ઓફ કોમર્સ એન્ડ ઈન્ડસ્ટ્રી

(આઇ. એસ. ઓ. ૯૦૦૧:૨૦૧૫ પ્રમાણિત સંસ્થા),

"સમૃધ્ધિ", ૪થો માળ, મક્કાઈ પુલ, નાનપુરા, સુરત – ૩૯૫ ૦૦૧

ફોન નં. ૨૨૯૧૧૧૧ ફેક્સ નં.૦૨૬૧–૨૪૭૨૩૪૦

E-mail : info@sgcci.in Website : www.sgcci.in

રેફ નં. તાઃ ૨૩/૪/૨૦૨૦

તંત્રીશ્રી, ____________________________, સુરત.

મે. સાહેબશ્રી,

જત નીચેની પ્રેસ નોટ આપના દૈનિકમાં પ્રસિદ્ધ કરી આભારી કરશોજ.

લિ.
આપનો વિશ્વાસુ,

(ખાતાકીય વડા)

ચેમ્બર દ્વારા 'બેસ્ટ સાયબર સિકયુરિટી પ્રેકટીસિસ ઇન કોરોના ક્રાઇસિસ' વિશે મહત્વનો વેબીનાર યોજાયો

સુરત. ધી સધર્ન ગુજરાત ચેમ્બર ઓફ કોમર્સ એન્ડ ઇન્ડસ્ટ્રી દ્વારા ગઇકાલે બપોરે ૧૨:૦૦ કલાકે 'બેસ્ટ સાયબર સિકયુરિટી પ્રેકટીસિસ ઇન કોરોના ક્રાઇસિસ' વિષય ઉપર વિડિયો કોન્ફરન્સ (વેબીનાર)નું આયોજન કરવામાં આવ્યુ હતુ. જેમાં એડવોકેટ, એટોર્ની એન્ડ સાયબર સિકયુરિટી કન્સલ્ટન્ટ ડો. ચિંતન પાઠક તેમજ ગુજરાત પોલીસના સ્કેચ મેકર અને સેફ સિટી સુરત કેમેરા પ્રોજેકટ કમિટીના સભ્ય શ્રી દિપેન જગીવાલાએ સાયબર સિકયુરિટી ઉપર મહત્વનું માર્ગદર્શન આપ્યુ હતુ. તેમણે ઓનલાઇન બેન્કીગ, ઇ–કોમર્સ અને ઝૂમ જેવી એપ્લીકેશનના ઉપયોગ વખતે શું કાળજી રાખવી તે વિશે સમજણ આપી હતી. ખાસ કરીને અજાણ્યા સાથે ઓટીપી અને કોડ કોઇપણ સંજોગોમાં શેર નહીં કરવા માટે તેમણે ચેતવ્યા હતા.

ચેમ્બરના પ્રમુખ શ્રી કેતન દેસાઇએ જણાવ્યુ હતુ કે, સોશિયલ મિડિયા ઉપર લોકો હેકર્સના શિકાર બની જતા હોય છે. અત્યારે કોવિડ માટે પીએમ કેરમાં ફંડ આપવા માટે ફેક ઇ–મેઇલ આઇડી પણ બની રહયા છે. હેકર્સ દ્વારા લોકોને છેતરવામાં આવી રહયાં છે. આવા સંજોગોમાં આપણે કયા પ્રકારની સાવચેતી રાખવી જોઇએ કે જેથી કરીને આપણું બેંક એકાઉન્ટ કે સોશિયલ મિડિયાનું એકાઉન્ટ હેક નહીં થાય તેના માટે આજના વેબીનારમાં વિશેષ માર્ગદર્શન મળી રહેશે.

ડો. ચિંતન પાઠકે જણાવ્યુ હતુ કે, ઉદ્યોગપતિ કે વેપારીઓના સાયબર ક્રાઇમના દરરોજ ઓછામાં ઓછા દસ કેસ સામે આવતા હોય છે. માલની એકસપ્રેસ ડિલીવરી માટે રૂપિયા દસ ટ્રાન્સફર કરવાનો હેકર્સ દ્વારા મેસેજ

મોકલવામાં આવે છે અને બેંકના ખાતામાંથી લાખો રૂપિયા ઉપાડી લેવામાં આવે છે. કેટલીક લોભામણી જાહેરાતોનો લોકો ભોગ બની જાય છે અને રૂપિયા ગુમાવી બેસે છે. વિદ્યાર્થીઓ તેમજ મહિલાઓનું ફેસબુક એકાઉન્ટ હેક થઇ જાય છે. અત્યારના સમયમાં પીએમ કેર ફંડના નામે ફેક આઇડી ફરતા થઇ ગયા છે. ઇએમઆઇ લંબાવવા માટે ઓટીપી શેર કરવા માટે ફોન આવે છે અને લોકોના ખાતામાંથી રૂપિયા સાફ થઇ જાય છે. અત્યારે પાંચ હજારથી વધુ ફેક ડોમેન બહાર ફરી રહયાં છે. જેમાં લોકો જોડાઇ જાય છે અને છેતરાઇ જાય છે. સોશિયલ મિડિયા ઉપર કોવિડ ૧૯ને લગતી કોઇપણ માહિતી મળે છે તો તેને કન્ફર્મ કર્યા વગર સકર્યુલેટ નહીં કરતા. આ ખૂબ જ ગંભીર ગુનો બને છે અને તમારી સામે એકશન પણ લેવાઇ શકે છે.

તેમણે વધુમાં જણાવ્યુ હતુ કે, હેકર માટે ગુજરાત સોફટ ટાર્ગેટ છે. સામાન્યપણે લોકો બીજાની વાતોમાં આવી જતા હોય છે. આઉટ ઓફ સ્ટેટના હેકર વધારે સાયબર ક્રાઇમ આચરે છે. ૨૪ કલાક સુધી એકશન નહીં લેવાય તો કશું કરી શકાતુ નથી. ડાયરેકટ સાયબર ક્રાઇમ પોલીસને ફરિયાદ આપી શકાય છે. સરકારની વેબસાઇટ cybercrime.gov.in ઉપર ફરિયાદ પણ ઓનલાઇન ફરિયાદ કરી શકાય છે. આપણે ટેકનોલોજીનો ઉપયોગ કરી રહયાં છે તેમ પ્રતિત થાય છે પણ હકીકતમાં ટેકનોલોજી આપણો ઉપયોગ કરે છે.

હેકર્સથી બચવા માટે આ બાબતોનું ખાસ ધ્યાન રાખો....

- પાસવર્ડ માટે મોબાઇલ નંબર અને નામ વિગેરેનો ઉપયોગ ન કરવો.
- ૧૨થી ૧૫ કેરેકટરનો પાસવર્ડ હોવો જોઇએ અને તેમાં પણ આલ્ફા ન્યુમરીકનો ઉપયોગ કરો.
- મોબાઇલફોનમાં ઓછામાં ઓછી એપ્લીકેશન રાખવી.
- ફાયનાન્શીયલ ટ્રાન્ઝેક્શન માટે જુદા મોબાઇલફોનનો ઉપયોગ કરો.
- કોઇપણ એપ્લીકેશન માટે માંગવામાં આવતા ઓટોપી અથવા કોડ ભૂલથી પણ શેર નહીં કરો.
- જે તે કંપનીની વેબસાઇડ પર જઇને ઇ–મેઇલ આઇડી અથવા તો ફોન પર સંપર્ક કરવો જોઇએ.
- ઝૂમ અથવા અન્ય એપ્લીકેશનના ઉપયોગ માટે જુદુ ઇ–મેઇલ આઇડી ક્રિએટ કરો.
- વર્ચ્યુઅલ પ્રાઇવેટ નેટવર્ક સર્વિસનો ઉપયોગ કરો. એમાં હેકર ઇ–મેઇલ આઇડી ટ્રેસ કરી શકે નહીં.
- પોપઅપ થતા એપ્લીકેશન ઉપર પોર્નોગ્રાફી કન્ટેન્ટ પણ લોડ થઇ જાય છે. આથી બાળકને ફોન આપો ત્યારે ફોનને મોનિટરીંગ કરો.
- કોઇપણ જાતના મેસેજ આવે એટલે સરકારની પ્રેસ ઇન્ફોર્મેશન બ્યુરો પીઆઇબી ફેક્ટ ચેક નામની વેબસાઇટ પર જઇને માહિતી સાચી છે કે કેમ તે પહેલા ચકાસો. ટોલ ફ્રી નંબર ૮૭૯૯૭૧૧૨૫૯ ઉપર પણ માહિતી ચેક કરી શકાય છે.
- ક્રેડીટ કાર્ડને બદલે ડેબીટ કાર્ડનો જ ઉપયોગ કરવો જોઇએ.
- નેટ બેન્કીગ માટે જુદુ એકાઉન્ટ ખોલાવો. એટલે કદાચ મોટું ફંડ ટ્રાન્સફર નહીં થઇ શકે.

શ્રી દિપેન જગીવાલાએ જણાવ્યુ હતુ કે, ઝૂમ એપ્લીકેશનના રજિસ્ટ્રેશન વખતે જે માહિતી આપતા હોય છે તેનુ તથા વેબીનાર કન્ટેન્ટનું ડાર્ક વેવ પર વેચાણ થઇ રહયુ હતુ. પાંચ લાખ ડેટાનુ વેચાણ થયા હોવાની માહિતી પણ મળી હતી. આથી સરકારે તેના ઉપયોગ અંગે એડવાઇઝરી જાહેર કરી હતી. આપણું હુંડીયામણ બહારના દેશમાં જઇ રહયું છે એટલે સરકારે આપણા દેશમાં જ આવી એપ્લીકેશન બનાવવાની જાહેરાત કરી છે. ઓનલાઇન એજયુકેશન માટે તેમજ લોકોને ઉપયોગી થનારા વેબીનાર માટે ઝૂમ એપ્લીકેશનના ઉપયોગમાં કોઈ

વાંધો આવતો નથી. કોર્પોરેટ સેકટર અને સરકારી વિભાગ ઉપયોગ કરે ત્યારે કોન્ફીડેન્શીયલ માહિતી જો એના પરથી લીક થાય તો મુશ્કેલી ઉભી થઇ શકે. એના માટે પણ ઘણી બધી સાવચેતી રાખવાની હોય છે.

ઝૂમ એપ્લીકેશનના ઉપયોગ માટે આ બાબતોનું ખાસ ઘ્યાન રાખો....

- જોઇન બીફોર હોસ્ટનુ ઓપ્શન ડિસેબલ રાખવુ.
- હોસ્ટ ઓનલીનુ ઓપ્શન સિલેકટ કરવુ.
- રીજોઇન કરવા માટે ઓપ્શન ડિસેબલ રાખવુ.
- જરૂરી નહીં હોય તો ફાઇલ ટ્રાન્સફરનુ ઓપ્શન ડિસેબલ રાખવુ.
- બધા પાર્ટીસિપેટ્સ જોઇન થાય તો મિટીંગને લોક કરવી જોઇએ.
- રેકોર્ડીગ કરો તો કોઇ વાંધો નહીં પણ કોન્ફીડેન્શીયલ માહિતી ચર્ચાતી હોય ત્યારે રેકોર્ડીગને ડિસેબલ કરી નાંખવું જોઇએ.

આર્થિક અને સામાજિક મુશ્કેલી ઉપર પ્રકાશ પાડતા તેમણે જણાવ્યુ હતુ કે હેકર તમારુ એકાઉન્ટ હેક કરીને સામાજિક પ્રતિષ્ઠાને હાનિ પહોંચાડે છે. સોશિયલ મિડિયા ઉપર તમારુ નામ અને તમારા ફોટા સાથે ડુપ્લીકેટ એકાઉન્ટ બનાવી તમને બદનામ કરી શકે છે. તમારો ચહેરો રામાયણના કયા પાત્ર જેવો દેખાય છે એવી ગેમ આવતી હોય તો ત્યારે પણ સાવચેત રહેવુ જોઇએ. અજાણી લીન્ક સાથે જોડાવવું નહીં જોઇએ. આર્થિક નુકસાન માટે લોભ, ભય અને ગેરસમજ કારણભુત થતા હોય છે. વોટ્સએપ ઉપર લોભામણી જાહેરાતો આવે છે અને લીન્ક ફરતી હોય છે. આવા સમયે લોકોએ પોતાની કોમન સેન્સ વાપરવાની હોય છે.

પેટ્રોલ પમ્પની બહાર ઉભા રહીને લોકો લકી ડ્રોની કૂપનમાં આપણી સંપૂર્ણ માહિતી ભરાવી લે છે. મોબાઇલ નંબર બંધ થઇ જશે વિગેરે ભય બતાવીને આપણી પાસે માહિતી માંગવામાં આવે છે. આપણી પાસે ઓટીપી માંગે એટલે આપણા ખાતામાંથી રૂપિયા ઉપાડીને આપણને છેતરી જાય છે. તમારી પોલિસી બંધ થઇ રહી છે અને ઓનલાઇન ચાલુ કરાવો વિગેરે ટ્રીક આવશે પણ તમારે સાવધાન રહેવુ પડશે. ભય કે લોભ બતાવવામાં આવે તો એવા કિસ્સામાં માહિતી નહીં આપો.

ઇ–કોમર્સમાં ઓએલએકસ પર પણ ઓછી કિંમતમાં ગાડીઓ મુકેલી હોય છે. થોડા રૂપિયા મોકલો અને પછી તમને ડિલીવરી કરવામાં આવશે વિગેરે બાબતોમાં સાવધાન રહેવાની જરૂર હોય છે. આપણા એકાઉન્ટ્સમાં રૂપિયા નથી આવતા પણ ટ્રાન્સફર થઇ જતા હોય છે. લોકો ગેરસમજને કારણે હેકરના ભોગ બની જાય છે. પેમેન્ટ સ્વીકારવા માટે કયારેય કયુઆર કોડ સ્કેન કરવામાં આવતો જ નથી. પેટીએમ પર પેમેન્ટ કરવા માટે જ કયુઆર કોડ સ્કેન કરવામાં આવે છે. આ બાબતને લોકોએ સમજવુ જોઇએ.

ગુગલ પેનો ઉપયોગ કરતા લોકોએ પણ ચેતવુ જોઇએ. જીયો પે કરીને આખી ફેક એપ્લીકેશન ઉપલબ્ધ છે. તમારા બેંક ખાતામાંથી ટ્રાન્ઝેકશન અટકાવવા માટે સૌથી પહેલા બેંકનો સંપર્ક કરવો જોઇએ અને ત્યારબાદ પોલીસનો કોન્ટેક કરવો જોઇએ. હેકરે તમારા બેંક ખાતામાંથી રૂપિયા ટ્રાન્સફર કરાવી લીધા હશે તો પણ હેકર રૂપિયા ઉપાડે એના પહેલા બેંકનો સંપર્ક કરી એના ખાતાને ફ્રીઝ કરી શકાય છે. હેકર કયારેક ઇ–કોમર્સ પ્લેટફોર્મ પરથી સીધી ખરીદી કરી લે છે. આવા સંજોગોમાં બેંકનો સંપર્ક કરી ઇ–કોમર્સનું એપ્લીકેશન માગી કોઇપણ ઇ–કોમર્સ ડિલીવરીને અટકાવી શકાય છે. આવા કિસ્સામાં અનુક્રમે બેંક, ઇ–કોમર્સ અને પોલીસનો

સંપર્ક કરવો જોઇએ. ટેકનોલોજીનો વ્યાપ વધી ગયો છે એટલે સાયબર ક્રાઇમની અવેરનેસ જરૂરી છે. એના માટે સમયસર એકશન લેવાય તો સારા પરીણામો મળી શકે છે.

ચેમ્બરના માનદ્ ખજાનચી શ્રી ધીરેન થરનારીએ વેબીનારનું સંચાલન કર્યુ હતુ. અંતે ચેમ્બરના ઇવેન્ટ્સ એન્ડ પ્રોગ્રામ્સ સેલના હેડ શ્રી મૃણાલ શુકલએ સર્વેનો આભાર માન્યો હતો અને ત્યારબાદ વેબીનારનું સમાપન થયુ હતુ.