સાયબર ઈન્શ્યોરન્સ

વ્યક્તિઓ માટે

અનુક્રમણિકા

1. સાયબર ઈન્સ્યોરન્સ શું છે?
2. કોને સાયબર વીમાની જરૂર છે
3. સાયબર પોલીસી કેમ લેવી જોઈએ...
4. કવરેજ
5. બાકાત (Exclusions)
6. વિવિધ મહત્વપૂર્ણ શરતો
7. ક્લેઈમ અંગે માહિતી

FINSURITA
SECURING FINANCIALS

સાયબર ઈન્સ્યોરન્સ શું છે

- સાયબર ઈન્સ્યોરન્સ, આપેલ સંદર્ભમાં, વીમા કવચ છે જે વીમાધારક વ્યક્તિ (વીમેદાર લાભાર્થી) ને અનધિકૃત ડિજિટલ નાણાકીય વ્યવહારને કારણે થતા કોઈપણ સીધા નાણાકીય નુકસાન સામે રક્ષણ આપે છે.
- અનધિકૃત ડિજિટલ નાણાકીય વ્યવહારનો અર્થ છે વીમાધારક લાભાર્થીના ખાતામાંથી તૃતીય પક્ષના ખાતામાં કપટપૂર્વક કરવામાં આવેલ કોઈપણ ઈલેક્ટ્રોનિક વ્યવહાર / ટ્રાન્સફર.

FINSURITA
SECURING FINANCIALS

તમારે સાયબર પોલીસી કેમ લેવી જોઈએ...

- દિવસે ને દિવસે સાયબર ફ્રોડના કિસ્સામાં થતો નોંધપાત્ર વધારો
- સાયબર છેતરપિંડી કરવા માટે સતત બદલાતી તકનીકો અને સાધનો
- સાયબર ફ્રોડ દ્વારા ગયેલા પૈસા પાછા આવવાની નહિવત તક
- આકર્ષક પ્રીમીયમના દર
- બધી જ જાતના સાયબર ફ્રોડનું એક જ પોલીસીમાં કવર મેળવો
- સરળતાથી પોલીસી ખરીદી શકાય છે
- સરળ ક્લેઈમ પ્રોસેસ છે

કોને સાયબર વીમાની જરૂર છે?

- પેમેન્ટ એપ ગ્રાહકો દા.ત. પેટીએમ, જીપે, ફોનપે, વગેરે.
- મોબાઈલ બેન્કિંગ/ફાઈનાન્સ એપ્લિકેશન ગ્રાહકો દા.ત. CitiMobile, iMobile, YONO, વગેરે.
- નેટ બેન્કિંગ ગ્રાહકો
- વ્યક્તિગત/વ્યવસાય રીમોટ વર્કીંગ – વર્ક ફ્રોમ હોમ
- ઈ-કોમર્સ ઉપભોક્તા
- એન્ટરપ્રીન્યોર્સ અને સ્ટાર્ટ અપ
- કનેક્ટેડ એન્વાયર્નમેન્ટ કન્ઝ્યુમર્સ એટલે કે સ્માર્ટ ઘડિયાળો, સ્માર્ટ ટીવી, પહેરવા યોગ્ય ગેજેટ્સ, સ્માર્ટ કિઓસ્ક વગેરે જેવા બહુવિધ ટચ પોઈન્ટ્સનો ઉપયોગ કરીને.

કવરેજ

અનધિકૃત ડિજિટલ ફાઈનાન્શિયલ ટ્રાન્ઝેક્શન: કોઈપણ ઈલેક્ટ્રોનિક ટ્રાન્ઝેક્શન/વીમેદાર લાભાર્થીના ખાતામાંથી તૃતીય પક્ષના ખાતામાં ટ્રાન્સફર, ઓળખની ચોરીના પરિણામે, નીચેના જોખમોમાંથી ઉદ્ભવતા (વીમેદાર/વીમેદાર લાભાર્થી દ્વારા પસંદ કરાયેલ)

- સાયબર હુમલા(ઓ)
- ફિશિંગ/સ્પૂફિંગ ઈ-મેલ અને/અથવા સંદેશાઓ અને/અથવા લિંક્સ અને/અથવા ટેલિફોનિક કૉલ્સ
- સિમજેકિંગ
- ઑનલાઈન ક્રેડિટ કાર્ડ / ડેબિટ કાર્ડ છેતરપિંડી

FINSURITA
SECURING FINANCIALS

સીધું નાણાકીય નુકસાન

- ડાયરેક્ટ ફાઈનાન્શિયલ લોસ એટલે કે પૈસાની પુનઃપ્રાપ્તિ ન થઈ શકે તેવી ખોટ
- વીમા ધારકના બેંક ખાતા અથવા પેમેન્ટ સીસ્ટમમાં રાખેલા ફંડ પર કંટ્રોલ મેળવી તેના દ્વારા નાણાની ઉચાપત

ખોટી ઓળખ આપી થતી છેતરપીંડી

પોલીસી ધારકને અજાણ્યા નામે ઓળખ આપી કપટ પૂર્ણ અથવા ખોટી રીતે થતી નાણાની ઉચાપત

સાયબર એટેક

સાયબર એટેક એ એવો દાવપેચ છે જ તમારી કોમ્પ્યુટર સીસ્ટમ, નેટવર્ક, ઈન્ફોર્મેશન, ડેટા અથવા સ્માર્ટ ફોનને લક્ષ્ય બનાવે છે. હુમલાખોર ખોટી રીતે ખોટા ઉદ્દેશ સાથે તમારા ડેટાને કંટ્રોલમાં લાવાનો પ્રયત્ન કરે છે. સાયબર એટેક તમારી સીસ્ટમને હેક કરીને ડેટા ને ચોરી શકે છે, બદલી શકે છે અથવા નાશ કરી શકે છે.

FINSURITA
SECURING FINANCIALS

ફિશિંગ/સ્પૂફિંગ

ફિશિંગ/સ્પૂફિંગ એટલે પોલિસી ધારકની સંવેદનશીલ માહિતી જેમ કે પાસવર્ડ, કાર્ડની વિગત, પૈસાની માહિતી વગેરે એક વિશ્વાસપાત્ર વ્યક્તિ તરિકે ઓળખ આપી ફ્રોડ કરવાની કોશીશ કરે છે.

સિમજેકિંગ

સિમજેકિંગ એટલે પોલીસી ધારકનું ટેલિકોમ કંપની દ્વારા આપવામાં આવેલું સીમકાર્ડ તેની જાણ અને સંમતિ વિના ફ્રોડ કરવાના ઈરાદાથી બદલી નાખવામાં આવે છે.

બાકાત (Exclusion)

- ATM માંથી નાણા ઉપાડવા તેમજ કોઈપણ ડીજીટલ વ્યવહારો
- કાર્ડ, ફોન, લેપટોપ ચોરી થયા પછી થતું નાણાકીય નુકશાન અથવા ફ્રોડ
- પોલીસી ધારકના પર્સનલ ડેટાને સાચવી રાખવામાં બેદરકારી દાખવવાથી થતું નુકશાન
- સાયબર એટેકથી વસુલી કરી થતું નુકશાન
- પોલીસી ધારક પોતે કરેલ છેતરપીંડી કે અપ્રમાણિકતા ના કારણે થતું નાણાકીય નુકશાન

FINSURITA
SECURING FINANCIALS

ક્લેઈમ સૂચના માટે સમય મર્યાદા

પોલિસી ધારકે નાણાકીય નુકશાનની જાણ થયાના 7 દિવસની અંદર વિમા કંપનીને જણાવવું જરુરી છે.

FINSURITA
SECURING FINANCIALS

ક્લેઈમની પ્રક્રિયા

ક્લેઈમ માટે ફરજિયાત દસ્તાવેજો

- સંપૂર્ણ રીતે ભરેલ ક્લેઈમ ફોર્મ
- પોલીસ સાયબર સેલની સાઈન વાળી E-FIR/FIR ની કોપી
- નાણાકીય સંસ્થાઓ સાથે નુકશાન બાબતે કરેલ પત્રવ્યવહારની નકલ
- એ દર્શાવવા માટેનો પુરાવો કે વીમાધારક લાભાર્થીને સીધું નાણાકીય નુકસાન વીમાધારક (બેંક/નાણાકીય સ્ટેટમેન્ટ) દ્વારા ઉઠાવવામાં આવ્યું છે તેની સાથે બેંકની સૂચના/પુષ્ટિ કે તેમના દ્વારા રકમ પરત કરવામાં આવશે નહીં

Thank You

FINSURITA
SECURING FINANCIALS

Mobile: 98252 29252, 99250 01811 • E-mail: Info@finsurita.com