કમ્પ્યૂટર સુરક્ષાનો પરિચય

પરિચય

કમ્પ્યૂટર આપણા દૈનિક જીવનનો એક ભાગ બની ગયું છે. આપણાં ઘણાં દૈનિક પુનરાવર્તિત કાર્યો કરવા માટે આપણે કમ્પ્યૂટરનો ઉપયોગ કરીએ છીએ. આપણો નોંધપાત્ર વ્યક્તિગત ડેટા જેમ કે ચિત્રો, આધાર કાર્ડની નકલ, બેંક વિગતો, શાળાના પ્રોજેક્ટ, અસાઈન્મેન્ટ, વગેરે આપણે ડેસ્કટોપ કમ્પ્યૂટર, લેપટોપ અને સ્માર્ટ ફોન જેવાં ઉપકરણો પર સંગ્રહિત કરીએ છીએ. આ ડેટાનો ઉપયોગ હેકર્સ જેવા લોકો તેમના અંગત ફાયદા માટે દુરુપયોગ કરી શકે છે. તેથી, આવા ડેટાને ગેરકાયદેસર ઉપયોગથી સુરક્ષિત રાખવો આપણા માટે મહત્ત્વપૂર્ણ છે. કમ્પ્યૂટર સુરક્ષાના મૂળભૂત સિદ્ધાંતો શીખીને આપણે કમ્પ્યૂટર સિસ્ટમ અને ડેટાને નુકસાન, ચોરી અને દુરુપયોગની સામે વધુ સારી રીતે સુરક્ષિત કરી શકીએ છીએ. આ પ્રકરણ કમ્પ્યૂટર સુરક્ષાના આવશ્યક ખ્યાલો શીખવામાં મદદ કરશે. આ પ્રકરણ દરમિયાન કમ્પ્યૂટર સુરક્ષાનું મહત્ત્વ, મુખ્ય સાઈબર જોખમો, મુખ્ય સુરક્ષા પદ્ધતિઓ અને ખાસ કરીને વિદ્યાર્થીઓ માટે રચાયેલ સામાન્ય કમ્પ્યૂટર સુરક્ષા માર્ગદર્શિકાઓ વિશે માહિતી મેળવીશું.

કમ્પ્યૂટર સુરક્ષાની જરૂરિયાત

આજે, આપણે વ્યક્તિગત ડેટાનો સંગ્રહ કરવા માટે કમ્પ્યૂટરના ઉપયોગ પર ખૂબ આધાર રાખીએ છીએ. જ્યારે આપણે કમ્પ્યૂટરનો ઉપયોગ કરીએ છીએ, ત્યારે ફક્ત આપણાં કાર્યો સંબંધિત સૉફ્ટવેર પર જ ધ્યાન કેન્દ્રિત કરીએ છીએ. જોકે, ત્યાં અન્ય ઘણા ઘટકો અને પ્રક્રિયાઓ બેકગ્રાઉન્ડમાં કાર્ય કરી રહ્યા હોય છે, જે ખાસ કરીને સુરક્ષાના દૃષ્ટિકોણથી નિર્ણાયક ભૂમિકા ભજવે છે. કમ્પ્યૂટર સિસ્ટમમાં વિવિધ ઉપયોગકર્તાઓ પણ સામેલ હોય છે.

આકૃતિ 11.1 : વર્તમાન કમ્પ્યૂટર સિસ્ટમમાં આવેલ પૂરક ઘટકો

જેમ કે, નિયમિત વપરાશકર્તાઓ તથા હેકર્સ, વાઇરસ અને વોર્મ્સ જેવા છુપાયેલા પ્રોગ્રામ. એન્ટીવાઇરસ સૉફ્ટવેર અને સિસ્ટમ સેટિંગ્સ જેવી સુરક્ષા સુવિધાઓ સિસ્ટમને સુરક્ષિત રાખવા માટે સતત કાર્ય કરી રહી હોય છે. કમ્પ્યૂટરની સર્વગ્રાહી સુરક્ષા સુનિશ્ચિત કરવા માટે આકૃતિ 11.1માં દર્શાવેલ આ તમામ ઘટકોને સમજવા ઘણા મહત્ત્વપૂર્ણ છે.

હેકર્સ દ્વારા દુરુપયોગથી આપણા ડિજિટલ સંસાધનોને સુરક્ષિત રાખવા માટે, મૂળભૂત કમ્પ્યૂટર સુરક્ષા તકનીકોને સમજવી આપણા માટે ખૂબ જ મહત્ત્વપૂર્ણ છે. ચાલો સમજીએ કે કમ્પ્યૂટરસુરક્ષા શા માટે મહત્ત્વપૂર્ણ છે અને સાઈબર હુમલાઓથી આપણા ડિજિટલ સંસાધનોને બચાવવા માટે આપણે શું કરી શકીએ.

કમ્પ્યૂટર સુરક્ષા શા માટે મહત્ત્વની છે?

કમ્પ્યૂટર સુરક્ષા આવશ્યક છે, કારણ કે આપણે શાળાનું કાર્ય, સોશિયલ મીડિયા પર વાતચીત, ઓનલાઈન બેંકિંગ, ખરીદી અને મનોરંજન જેવી રોજિંદી પ્રવૃત્તિઓ માટે ટેકનોલોજી પર નિર્ભર છીએ. કમ્પ્યૂટર સુરક્ષા વિશે શીખીને, આપણે આપણી વ્યક્તિગત અને સંવેદનશીલ માહિતીને સુરક્ષિત કરી શકીએ છીએ, અને સલામત ડિજિટલ વાતાવરણ બનાવી શકીએ છીએ.

કમ્પ્યૂટર સુરક્ષાનો ઉદ્‌ભવ

કમ્પ્યૂટરના ઉપયોગના પ્રારંભિક દિવસોમાં કમ્પ્યૂટર સુરક્ષાનો ખ્યાલ કોઈ ચિંતાનો વિષય ન હતો. શરૂઆતમાં, કમ્પ્યૂટર મોટાં, અલગ (isolated) મશીનો હતાં, જેનો ઉપયોગ મર્યાદિત વ્યક્તિઓ દ્વારા થતો હતો. જો કે, જેમ જેમ ટેકનોલૉજીનો વિકાસ થયો અને એકબીજા સાથે જોડાયેલ (interconnected) કમ્પ્યૂટર સિસ્ટમ અસ્તિત્વમાં આવી, તેમ તેમ સુરક્ષાની જરૂરિયાત સ્પષ્ટ થઈ. 20મી સદીના ઉત્તરાર્ધમાં ઈન્ટરનેટનો વિકાસ એક વિશિષ્ટ ઘટના હતી, કારણ કે તેણે નવી તકોની સાથે પડકારો પણ ઊભા કર્યા.

સાઈબર સુરક્ષાનો વિકાસ (The Evolution of Cybersecurity)

આજકાલ, કમ્પ્યૂટર સુરક્ષાને સામાન્ય રીતે સાઈબર સુરક્ષા (Cybersecurity) તરીકે ઓળખવામાં આવે છે. આ ક્ષેત્ર કમ્પ્યૂટર, સ્માર્ટફોન, નેટવર્ક અને ડેટાને હેકર્સ તરીકે ઓળખાતા હુમલાખોરો દ્વારા થતા અનધિકૃત પ્રવેશ (unauthorized access)થી બચાવવા પર ધ્યાન કેન્દ્રિત કરે છે. સાઈબર સુરક્ષાનો વિકાસ કમ્પ્યૂટર નેટવર્કના ઉદય સાથે શરૂ થયો હતો. 1990ના દાયકામાં ઈન્ટરનેટનો વપરાશ વધ્યો તેમ, વાઈરસ, વોર્મ્સ અને હેકિંગ જેવી સાઈબર જોખમો વધુ સામાન્ય બન્યાં. ઈન્ટરનેટના ઉપયોગથી નવા પ્રકારના પડકારો આવ્યા. વાઈરસ જેવા કમ્પ્યૂટર આધારિત દૂષિત પ્રોગ્રામ્સ ઘણા ઈન્ટરનેટ વપરાશકર્તાઓ માટે સમસ્યાઓ ઊભી કરવા લાગ્યા. આનાથી સાઈબર સુરક્ષાનો જન્મ થયો, જે એક એવું ક્ષેત્ર છે જે વિવિધ પ્રકારની સાઈબર સમસ્યાઓ સામે રક્ષણ આપવા માટે વ્યૂહરચનાઓ અને તકનીકો વિકસાવવા માટે સમર્પિત છે.

મહત્ત્વપૂર્ણ ડિજિટલ સંસાધનો

કમ્પ્યૂટર સુરક્ષાના સંદર્ભમાં, 'ડિજિટલ સંસાધનો' એટલે એવી કોઈપણ વસ્તુ જે ડિજિટલ ફોર્મેટમાં અસ્તિત્વમાં હોય અને તેનું ચોક્કસ મૂલ્ય હોય, જેને અનધિકૃત પ્રવેશ અથવા હુમલાઓથી સુરક્ષિત રાખવાની જરૂર હોય. ટેબલ 11.1 કેટલાક મુખ્ય ડિજિટલ સંસાધનોની રૂપરેખા આપે છે જેને વ્યક્તિઓ, શાળાઓ, સરકારો અને વ્યવસાયોએ સંભવિત હુમલાખોરો સામે સુરક્ષિત રાખવાની જરૂર છે.

શ્રેણી	સુરક્ષા જરૂરી હોય તેવા ડિજિટલ સંસાધનો
વ્યક્તિગત	ફોન નંબર, રહેઠાણનું સરનામું, ઈમેઈલ એડ્રેસ, બેંક ખાતા નંબરો, ડેબિટ/ક્રેડિટ કાર્ડની વિગતો, UPI IDs, ઓળખ કાર્ડ (આધાર, PAN, પાસપોર્ટ, ડ્રાઈવિંગ લાઈસન્સ), વ્યક્તિગત ફોટોગ્રાફ્સ અને વીડિયો, બાયોમેટ્રિક વિગતો (ફિંગરપ્રિન્ટ્સ, ફેસ ID), સોશિયલ મીડિયા એકાઉન્ટ આઈડી, વગેરે.
શાળા	વિદ્યાર્થી અને શિક્ષકના સંપર્કની વિગતો, હાજરીના રેકોર્ડ, શૈક્ષણિક પરિણામો, ડિજિટલ પ્રશ્નપત્રો અને જવાબવહીઓ, ઈ-લર્નિંગ પ્લેટફોર્મ, એપ્સ અને તેમના યુઝરનેમ પાસવર્ડ, શાળાની વેબસાઈટ, ફી ચૂકવણીનો ડેટા, શાળાના નેટવર્ક અને Wi-Fi પાસવર્ડ્સ, વગેરે.
સરકાર	આધાર અને અન્ય ID ડેટાબેઝ, ચૂંટણીના રેકોર્ડ, આવકવેરાના રેકોર્ડ, આરોગ્ય ડેટા, પાસપોર્ટ/ઈમિગ્રેશન ડેટા, રેશનકાર્ડ, પેન્શન, જમીન અને મિલકતના રેકોર્ડ, ડિજિટલ નકશાઓ, સંરક્ષણ સંબંધિત ગુપ્ત માહિતી વગેરે.
વ્યવસાય	બેંકવિગતો, ગ્રાહક ડેટા (નામ, ઈમેઈલ, ફોન નંબર), કર્મચારી રેકોર્ડ અને પગારની વિગતો, વ્યવસાયિક ઈમેઈલ, વેબસાઈટ અને એપ્સ, લોન/રોકાણની વિગતો, વ્યવસાયિક રહસ્યો, વિક્રેતાની વિગતો, વગેરે.

ટેબલ 11.1 : મહત્ત્વના ડિજિટલ સંસાધનો

આ તમામ ડિજિટલ સંસાધનોને માત્ર હેકર્સથી જ નહીં, પણ આકસ્મિક નુકસાન, કર્મચારીઓ દ્વારા આંતરિક હુમલાઓ, વ્યવસાયિક સ્પર્ધકો અને આંતરરાષ્ટ્રીય હુમલાઓથી પણ સુરક્ષાની જરૂર છે.

ડેટા પ્રાઇવસી અને સુરક્ષા

ડેટા પ્રાઇવસી અને સુરક્ષા વિશે સમજણ મેળવવી આપણા માટે ખૂબ જ મહત્ત્વપૂર્ણ છે, ખાસ કરીને એ કારણથી કે આપણે દૈનિક જીવનમાં સ્માર્ટ ફોન પર ખૂબ જ આધાર રાખીએ છીએ.

વ્યક્તિગત માહિતી, જેમ કે નામ, સરનામાં અને શાળાના રેકોર્ડને અનધિકૃત ઍક્સેસ અને દુરુપયોગ સામે સુરક્ષિત રાખવાની પ્રથાને ડેટા પ્રાઇવસી કહે છે. પ્રાઇવસી જાળવવા અને માહિતી ખોટા હાથોમાં ન જાય તે સુનિશ્ચિત કરવા માટે આ ડેટાનું રક્ષણ કરવું મહત્ત્વપૂર્ણ છે.

વિદ્યાર્થીઓ માટે ડેટા પ્રાઇવસી શા માટે મહત્ત્વની છે?

વિદ્યાર્થીઓ માટે ડેટા પ્રાઇવસીને સમજવી મહત્ત્વપૂર્ણ છે કારણ કે તેઓ મોટેભાગે આકર્ષક ઇન્ટરનેટ વિશ્વની અંધારી બાજુ વિશે જાગૃત હોતા નથી. ડેટા પ્રાઇવસી જાળવવાથી ઓળખ અને વ્યક્તિગત માહિતીને સાઇબર અપરાધીઓથી સુરક્ષિત રાખવામાં મદદ મળે છે જેઓ તેનો દૂષિત હેતુઓ માટે ઉપયોગ કરવાનો પ્રયાસ કરી શકે છે. ડેટા પ્રાઇવસી વિશે જાગૃત રહેવાનો અર્થ છે :

- તમે ઓનલાઇન શું શેર કરો છો તે વિશે સાવચેત રહેવું.
- આપણા સોશિયલ મીડિયા એકાઉન્ટ પરની પ્રાઇવસી સેટિંગ્સ (privacy settings)ને સમજવું.
- મજબૂત અને અનન્ય પાસવર્ડના મહત્ત્વને ઓળખવું.

ડેટા સુરક્ષામાં શાળાઓ અને વિદ્યાર્થીઓની ભૂમિકા

વિદ્યાર્થીઓની માહિતીનું સંચાલન કરવા માટે સુરક્ષિત સિસ્ટમો લાગુ કરીને, નિયમિત સુરક્ષા ઓડિટ કરીને, અને વિદ્યાર્થીઓને જવાબદાર ઓનલાઇન વર્તન વિશે શિક્ષિત કરીને શાળાઓ ડેટા સુરક્ષામાં નિર્ણાયક ભૂમિકા ભજવે છે.

વિદ્યાર્થીઓ તરીકે, તમે ડેટા સુરક્ષામાં નીચે મુજબ યોગદાન આપી શકો છો :

- તમે જે માહિતી શેર કરો છો તેના વિશે સાવધ રહેવું.
- સુરક્ષિત Wi-Fi નેટવર્કનો ઉપયોગ કરવો.
- કોઈપણ શંકાસ્પદ પ્રવૃત્તિઓની જાણ કોઈ વિશ્વાસપાત્ર પુખ્ત વ્યક્તિ અથવા તમારા શિક્ષકને કરવી.

ડેટા પ્રાઇવસી અને સુરક્ષા તકનીકો વિશે પોતાને શિક્ષિત કરીને, વિદ્યાર્થીઓ તેમના અને તેમના પરિવારના સભ્યો માટે વધુ સુરક્ષિત ડિજિટલ વાતાવરણ બનાવવામાં મદદ કરી શકે છે.

સાઇબર સુરક્ષાનો પરિચય

સાઇબર સુરક્ષામાં કમ્પ્યૂટર, સ્માર્ટફોન, નેટવર્ક અને ડેટાને અનધિકૃત પ્રવેશથી સુરક્ષિત રાખવાનો સમાવેશ થાય છે. તે સુનિશ્ચિત કરે છે કે આપણે જે ડિજિટલ માહિતીનો ઉપયોગ કરીએ છીએ અને શેર કરીએ છીએ તે હેકર્સ અને વાઇરસ જેવાં જોખમોથી સુરક્ષિત છે. વિદ્યાર્થીઓ માટે સાઇબર સુરક્ષાનો અર્થ છે વ્યક્તિગત માહિતીને કેવી રીતે સુરક્ષિત રાખવી તે શીખવું અને સંભવિત ઓનલાઇન જોખમો વિશે જાગૃત રહેવું તથા મજબૂત પાસવર્ડ તેમજ સલામત ઓનલાઇન પ્રથાઓનું મહત્ત્વ સમજવું. સાઇબર સુરક્ષાના મૂળભૂત સિદ્ધાંતોને સમજીને, વિદ્યાર્થીઓ ડિજિટલ વિશ્વમાં સુરક્ષિત રીતે સર્ફ કરી શકે છે, સુરક્ષિત ઓનલાઇન પ્રવૃત્તિઓમાં જોડાઈ શકે છે અને પોતાને તથા તેમના સમુદાયોને સુરક્ષિત કરવા માટેની કુશળતા વિકસાવી શકે છે.

સાઇબર સુરક્ષાનાં કરવાયોગ્ય (Do's) અને ન કરવા યોગ્ય મૂળભૂત (Don'ts) કાર્યો

ડિજિટલ વિશ્વમાં આપણી સલામતી અને પ્રાઇવસીનું રક્ષણ કરવા માટે અસરકારક સાઇબર સુરક્ષાની આદતોને સમજવી અને તેને અમલમાં મૂકવી આપણા માટે આવશ્યક છે. ટેબલ 11.2માં આપેલી મૂળભૂત કરવા યોગ્ય (Do's) અને ન કરવા યોગ્ય (Don'ts) બાબતોનું પાલન કરીને, આપણે સાઇબર-હુમલાઓનો ભોગ બનવાની શક્યતાઓને મોટા પ્રમાણમાં ઘટાડી શકીએ છીએ.

પાસું	કરવા યોગ્ય (Do's)	ન કરવા યોગ્ય (Don'ts)
અંગત માહિતી	તમારો ડેટા સોશિયલ મીડિયા પ્લેટફોમ પર ખાનગી રાખો. જો જરૂરી હોય, તો ઓછામાં ઓછો ડેટા શેર કરો.	સોશિયલ મીડિયા અને સાર્વજનિક વેબ-સાઈટ પર તમારું પૂરું નામ, સરનામું, ફોન નંબર અને જન્મ તારીખ પોસ્ટ કરવાનું ટાળો.
યુઝર આઈડી	જ્યાં શક્ય હોય ત્યાં, દરેક ઓનલાઈન એકાઉન્ટ માટે અલગ-અલગ યુઝર આઈડી (વપરાશકર્તા નામ)નો ઉપયોગ કરો.	તમારા ઈમેઈલ એડ્રેસનો ઉપયોગ યુઝરનેમ તરીકે કરવાનું ટાળો, કારણ કે તે હુમલાખોરોને તમારા અન્ય ઓનલાઈન એકાઉન્ટ શોધવામાં મદદ કરે છે.
પાસવર્ડ	દરેક એકાઉન્ટ માટે મજબૂત અને અનન્ય પાસવર્ડનો ઉપયોગ કરો. મજબૂત પાસવર્ડ બનાવવા માટે, અપરકેસ અને લોઅરકેસ અક્ષરો, સંખ્યાઓ અને પ્રતીકોનું સંયોજન વાપરો. ઉદાહરણ તરીકે, “P@ndas$5Rocks” એક મજબૂત પાસવર્ડ છે.	તમારું નામ, જન્મદિવસ અથવા "abc123" જેવા સરળતાથી અનુમાન લગાવી શકાય તેવા પાસવર્ડનો ક્યારેય ઉપયોગ કરશો નહીં. બહુવિધ એકાઉન્ટ માટે સમાન પાસવર્ડનો ઉપયોગ કરશો નહીં. કાગળ પર પાસવર્ડ લખવાનું ટાળો. “panda123” એ નબળા પાસવર્ડનું ઉદાહરણ છે.
ટુ ફેક્ટર ઓથેન્ટિકેશન (2FA)	તમારા તમામ એકાઉન્ટ પર, ખાસ કરીને ઈમેઈલ, બેંકિંગ અને સોશિયલ મીડિયા એકાઉન્ટ પર, 2FA (ટૂ-ફેક્ટર ઓથેન્ટિકેશન - Two-Factor Authentication) સક્ષમ કરો.	તમારા 2FA કોડ જેમ કે વન-ટાઈમ-પાસવર્ડ (OTP) કોઈની પણ સાથે ક્યારેય શેર કરશો નહીં.
પબ્લિક Wi-Fi	પબ્લિક Wi-Fi નો ઉપયોગ કરતી વખતે ફક્ત HTTPS સાઈટ્સને જ એક્સેસ કરો. તેમજ, ખાતરી કરો કે તમારું ઘરનું Wi-Fi પાસવર્ડ-સુરક્ષિત છે.	પબ્લિક Wi-Fiનો ઉપયોગ કરતી વખતે બેંકિંગ અથવા શોપિંગ એકાઉન્ટનો ઉપયોગ કરવાનું ટાળો. અજાણ્યા Wi-Fi નેટવર્ક સાથે કનેક્ટ થવાનું ટાળો. હેકર્સ આપણો ડેટા ચોરી શકે છે.
સૉફ્ટવેર અપડેટ્સ	ઓપરેટિંગ સિસ્ટમ, વેબ બ્રાઉઝર અને એપ્સ માટેના સૉફ્ટવેર અપડેટ ઉપલબ્ધ થતાંની સાથે જ ઈન્સ્ટોલ કરો.	સૉફ્ટવેર અપડેટની ચેતવણીઓને અવગણશો નહીં.
લિંક અને ઈમેઈલ	કોઈપણ લિંક અથવા એટેચમેન્ટ ખોલતાં પહેલાં મોકલનારની વિગતો ચકાસો. લિંક પર ક્લિક કરતા પહેલાં તેનું ખરેખરું URL જોવા માટે તેની પર માઉસ ફેરવો.	અજાણ્યા SMS અને ઈમેઈલ મોકલનારાઓ તરફથી આવતી લિંક પર ક્લિક કરવાનું ટાળો, અને અજાણી વિનંતીઓના જવાબમાં વ્યક્તિગત ડેટા શેર કરશો નહીં.
એપ ડાઉનલોડ	માત્ર Google Play Store અને Apple App Store જેવા અધિકૃત એપ સ્ટોર પરથી જ એપ્સ ડાઉનલોડ કરો.	ત્રાહિત સ્રોતમાંથી ક્યારેય એપ્સ અથવા .APK ફાઈલ ડાઉનલોડ કરશો નહીં. કોઈપણ એપ્સને બિનજરૂરી પરવાનગીઓ આપશો નહીં (દા.ત.,

		એક ફ્લેશલાઇટ એપ તમારા સંપર્કોને ઍક્સેસ કરવાની વિનંતી કરે).
સિક્યોરીટી એલર્ટ	ઓપરેટિંગ સિસ્ટમ અને એન્ટીવાઇરસ સૉફ્ટવેર તરફથી આવતી સુરક્ષા ચેતવણીઓ પર ધ્યાન આપો અને તેના પર તાત્કાલિક પગલાં લો.	સંભવિત જોખમોને સમજ્યા વિના કોઈપણ સુરક્ષા ચેતવણીઓને ક્યારેય રદ કરશો નહીં કે અવગણશો નહીં.
બેકઅપ	મહત્ત્વપૂર્ણ ડેટા ફાઇલોનો નિયમિત બેકઅપ લો. બેકઅપને અલગ-અલગ જગ્યાએ સંગ્રહિત કરો (દા.ત., ક્લાઉડ, બાહ્ય રિસ્ક અને પેન ડ્રાઇવ).	બેકઅપ લીધા પછી બેકઅપ ડ્રાઇવને કમ્પ્યૂટરથી અલગ કરો. તેને જોડાયેલું રાખશો નહીં.
સાઇબર બુલિંગ	જો સાઇબરબુલિંગનો સામનો કરવો પડે, તો તેની જાણ શિક્ષક અને માતા-પિતાને કરો.	સાઇબરબુલીઝને જવાબ આપીને કે પ્રતિક્રિયા આપીને તેમની સાથે જોડાશો નહીં.
શંકાસ્પદ પ્રવૃત્તિ	તમારા એકાઉન્ટ અથવા ઉપકરણો પરની કોઈપણ શંકાસ્પદ પ્રવૃત્તિની જાણ તાત્કાલિક તમારા શિક્ષક અને તમારા માતા-પિતાને કરો.	ઓનલાઈન એકાઉન્ટમાં કોઈપણ અસામાન્ય લોગિન પ્રયાસો અથવા ખૂબ જ નાના નાણાકીય વ્યવહારોને અવગણશો નહીં.

ટેબલ 11.2 : સાઇબર સુરક્ષાના મૂળભૂત કરવા યોગ્ય (Do's) અને ન કરવા યોગ્ય (Don'ts) કાર્યો

વિદ્યાર્થીઓ માટે સલામત બ્રાઉઝિંગની આદતો

ઇન્ટરનેટ વેબસાઇટ પર સુરક્ષિત રીતે નેવિગેટ કરવું તે આપણા બધા માટે આપણી વ્યક્તિગત માહિતીનું રક્ષણ કરવા અને ઓનલાઈન પ્રાઇવસી જાળવવા માટે ખૂબ જ મહત્ત્વપૂર્ણ છે.

સલામત બ્રાઉઝિંગની આદતો વિશે જાગૃત રહેવાથી આપણને માલવેર અને ફિશિંગ જેવા સાઇબર જોખમોને ટાળવામાં મદદ મળે છે. સલામત બ્રાઉઝિંગ માટેની કેટલીક મુખ્ય પ્રથાઓ નીચે મુજબ છે :

- **નવીનતમ વેબ બ્રાઉઝરનો ઉપયોગ કરો :** સુરક્ષાની નવીનતમ સુવિધાઓ અને પેચ (patches) નો લાભ લેવા માટે તમારા વેબ બ્રાઉઝરને હંમેશા નવીનતમ આવૃત્તિ પર અપડેટ રાખો.
- **HTTPS જુઓ :** વેબસાઇટની મુલાકાત લેતી વખતે, ખાતરી કરો કે તેઓ URL માં **"HTTPS"** નો ઉપયોગ કરે છે, જે સુરક્ષિત કનેક્શન સૂચવે છે અને આપણો ડેટા એન્ક્રિપ્ટેડ (encrypted) છે.
- **અજાણી લિંક્સ પર ક્લિક કરવાનું ટાળો :** અજાણ્યા સ્રોતોમાંથી ઈમેઈલ અથવા સંદેશાઓમાં શેર કરેલી લિંક્સ વિશે સાવચેત રહો. ક્લિક કરતા પહેલા URLનું પૂર્વાવલોકન (preview) કરવા માટે લિંક પર માઉસ ફેરવો.
- **પોપ-અપ બ્લોકરનો ઉપયોગ કરો :** સંભવિત હાનિકારક પોપ-અપ જાહેરાતો (pop-up ads) ને દેખાતી અટકાવવા માટે બ્રાઉઝર સેટિંગ્સમાં પોપ-અપ બ્લોકર (Pop-up Blocker) ને સક્ષમ કરો.
- **મફત ઓફર વિશે શંકાશીલ બનો :** મફત ડાઉનલોડ અથવા ભેટ ઓફર કરતી વેબસાઇટથી સાવધ રહો, કારણ કે તેમાં ઘણીવાર માલવેર હોય છે અથવા તે ફિશિંગ સાઇટ તરફ દોરી જાય છે.
- **એકાઉન્ટમાંથી લોગઆઉટ કરો :** અનધિકૃત પ્રવેશ અટકાવવા માટે વહેંચાયેલ (shared) અથવા સાર્વજનિક (public) કમ્પ્યૂટરનો ઉપયોગ કરતી વખતે હંમેશા ઓનલાઈન એકાઉન્ટમાંથી લોગઆઉટ કરો.
- **નિયમિતપણે કૂકીઝ અને કેશ સાફ કરો :** તમારી પ્રાઇવસીને સુરક્ષિત રાખવા અને બ્રાઉઝરનું પ્રદર્શન સુધારવા માટે તમારા બ્રાઉઝરની કૂકીઝ (cookies) અને કેશ (cache) નિયમિતપણે સાફ કરો.

વિદ્યાર્થીઓ આ સલામત બ્રાઉઝિંગની આદતો અપનાવીને સાઇબર હુમલાઓના જોખમોને ઓછામાં ઓછા કરી શકે છે અને ઇન્ટરનેટનો સુરક્ષિત રીતે આનંદ માણી શકે છે.

સાઇબર જોખમોનો પરિચય

સાઇબર જોખમ (cyber threat)ને ડેટા, ડિજિટલ સિસ્ટમ અને નેટવર્કને નુકસાન પહોંચાડવા, ચોરી કરવા અથવા વિક્ષેપિત કરવાના હેતુથી કરવામાં આવતી કોઈપણ હાનિકારક કાર્યવાહી તરીકે વ્યાખ્યાયિત કરવામાં આવે છે. મૂળભૂત રીતે, તે સફળ સાઇબર હુમલાની સંભાવના દર્શાવે છે.

તેથી, આપણા કમ્પ્યૂટર અને વ્યક્તિગત માહિતીને નુકસાન પહોંચાડી શકે તેવા જોખમો વિશે આપણે જાણવું જરૂરી છે. ચાલો આપણે તેની લાક્ષણિકતાઓ અને કેટલાક સામાન્ય સાઇબર જોખમો ને સમજીએ.

સાઇબર જોખમોની મુખ્ય લાક્ષણિકતાઓ

- **સાઇબર જોખમકર્તાઓ (Cyber Threat Actors) :** તેઓ હેકર્સ તરીકે જાણીતા છે જેઓ દૂષિત ઇરાદો ધરાવે છે. તેઓ અનધિકૃત પ્રવેશ મેળવવા માટે સિસ્ટમની નબળાઈઓનો દુરુપયોગ કરવાનો હેતુ ધરાવે છે અને પછી પીડિતોના ડેટા, ઉપકરણો, સિસ્ટમ અને નેટવર્કનો દુરુપયોગ કરે છે.
- **દૂષિત ઇરાદો (Malicious Intent) :** તે સામાન્ય રીતે વ્યક્તિઓ અથવા જૂથો (હેકર્સ) દ્વારા નાણાકીય અથવા બિન-નાણાકીય લાભો જેવા હાનિકારક ઇરાદાઓ સાથે હાથ ધરવામાં આવે છે.
- **નબળાઈઓને લક્ષ્ય બનાવવું (Targeting Vulnerabilities) :** જોખમકર્તાઓ માહિતી પ્રણાલીઓ, સૉફ્ટવેર, હાર્ડવેર અથવા તો માનવ વર્તનમાં રહેલી નબળાઈઓ અથવા ખામીઓનો લાભ ઉઠાવે છે.
- **પ્રાઇવસી, અખંડિતતા અને ઉપલબ્ધતા (CIA Triad) પર અસર (Impact on Confidentiality, Integrity and Availabilty) :** સાઇબર જોખમો આ મુખ્ય સુરક્ષા સિદ્ધાંતોમાંથી એક અથવા વધુને જોખમમાં મૂકવાનો હેતુ ધરાવે છે :
    - પ્રાઇવસી (Confidentiality): સંવેદનશીલ માહિતીનો અનધિકૃત ઉપયોગ.
    - અખંડિતતા (Integrity): ડેટામાં અનધિકૃત ફેરફાર અથવા નાશ.
    - ઉપલબ્ધતા (Availability): સિસ્ટમ અથવા ડેટાની ઍક્સેસમાં વિક્ષેપ (દા.ત., ડિનાયલ ઓફ સર્વિસ એટક - Denial of Service attacks).

તમે તમારા ઉચ્ચ ધોરણોમાં CIA ટ્રાયડ વિશે વધુ શીખશો.

સાઇબર જોખમોના પ્રકારો

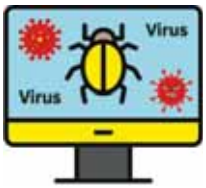
ચાલો સાઇબર જોખમોના સામાન્ય પ્રકારોને સમજીએ.

માલવેર (Malware)

માલવેર એ એક પ્રકારનું સૉફ્ટવેર છે જે કમ્પ્યૂટર સિસ્ટમને નુકસાન પહોંચાડવા અથવા તેમાં અનધિકૃત પ્રવેશ મેળવવા માટે રચાયેલું છે. માલવેર એક સામાન્ય શબ્દ છે જેનો ઉપયોગ વાઇરસ, વોર્મ્સ, ટ્રોજન (Trojans) વગેરે જેવા તમામ પ્રકારના દૂષિત સૉફ્ટવેરનો ઉલ્લેખ કરવા માટે થાય છે. ઇમેઇલ એટેચમેન્ટ અથવા અવિશ્વસનીય વેબસાઇટ્સ પરથી ડાઉનલોડ કરેલી ફાઇલોમાં માલવેર છુપાયેલું હોઈ શકે છે.

માલવેરને વાઇરસ, વોર્મ્સ, ટ્રોજન, રેન્સમવેર, સ્પાયવેર, એડવેર અને કી-લોગર્સ જેવા વિવિધ પ્રકારોમાં વર્ગીકૃત કરી શકાય છે. હેકર્સ દ્વારા સાઇબર હુમલાઓ કરવા માટે આનો સામાન્ય રીતે ઉપયોગ થાય છે.

વાઇરસ (Virus)



વાઇરસ એ હાનિકારક પ્રોગ્રામ છે જે એક કમ્પ્યૂટરમાંથી બીજા કમ્પ્યૂટરમાં ફેલાઈ શકે છે. તેઓ ફાઇલો અને પ્રોગ્રામ સાથે પોતાને જોડે છે, જેના કારણે તે ધીમા ચાલે છે અથવા બિલકુલ ચાલતા નથી. વાઇરસ તમારા કમ્પ્યૂટરમાંથી મહત્ત્વપૂર્ણ ડેટા ફાઇલો અને વ્યક્તિગત માહિતીને ભ્રષ્ટ (corrupt) અથવા ડિલીટ પણ કરી શકે છે.

વોર્મ (Worm)

વોર્મ એ એક પ્રકારનું સ્વ-પ્રતિકૃતિ (self-replicating) માલવેર છે, જે વપરાશકર્તાની કોઈપણ ક્રિયા વિના કમ્પ્યૂટર અને નેટવર્ક પર ફેલાય છે. વાઇરસથી વિપરીત, વોર્મને હોસ્ટ પ્રોગ્રામ અથવા ફાઇલ સાથે પોતાને જોડવાની જરૂર નથી.

ટ્રોજન (Trojan)

ટ્રોજન એ એક પ્રકારનું દૂષિત સૉફ્ટવેર છે જે કાયદેસર સૉફ્ટવેર અથવા ફાઇલ જેવું દેખાય છે. ટ્રોજન ઘણીવાર રમતો, યુટિલિટીઝ અથવા ઈમેઈલ એટેચમેન્ટ જેવા મદદરૂપ સૉફ્ટવેર તરીકે પોતાને રજૂ કરે છે. એકવાર સક્રિય થયા પછી, તે વપરાશકર્તાની જાણ વગર વિવિધ હાનિકારક ક્રિયાઓ કરી શકે છે.

રેન્સમવેર (Ransomware)

રેન્સમવેર એ એક પ્રકારનું હાનિકારક સૉફ્ટવેર છે જે તમારા ડેટાને લૉક એન્ક્રિપ્ટ કરે છે, જેનાથી તે અનુપયોગી બની જાય છે. તે આપણું કમ્પ્યૂટર પણ લૉક કરી શકે છે. પછી હુમલાખોર તેને અનલૉક કરવા માટે ખંડણીની માંગ કરે છે. તે ઘણીવાર નકલી ઈમેઈલ અથવા અસુરક્ષિત ડાઉનલોડ દ્વારા ફેલાય છે. ખંડણી ચૂકવવાથી હંમેશા ખાતરી મળતી નથી કે તમારો ડેટા અથવા કમ્પ્યૂટરનો વપરાશ હુમલાઓમાંથી પુનઃ પ્રાપ્ત થશે.

સ્પાયવેર (Spyware)

સ્પાયવેર એ એક પ્રકારનું માલવેર છે જે વપરાશકર્તાની તેમના કમ્પ્યૂટર અથવા મોબાઈલ સાધન પરની પ્રવૃત્તિઓ વિશેની માહિતીને ગુપ્ત રીતે નિહાળવા અને એકત્રિત કરવા માટે રચાયેલું છે.

એડવેર (Adware)

એડવેર એ એક પ્રકારનું સૉફ્ટવેર છે જે ઘણીવાર વપરાશકર્તાની સંમતિ વિના, વપરાશકર્તાના ઉપકરણ પર અનિચ્છનીય જાહેરાતો આપમેળે પ્રદર્શિત કરે છે. તેઓ હંમેશા દૂષિત હોતા નથી, પરંતુ તે તમારી સિસ્ટમને ધીમું કરી શકે છે, ઇન્ટરનેટ બેન્ડવિડ્થ વાપરી શકે છે અને આપણી પ્રાઇવસીને જોખમમાં મૂકી શકે છે.

કી-લોગર્સ (Keyloggers)

કી-લોગર્સ એવા પ્રોગ્રામ છે જે આપણા કીબોર્ડ પર કરવામાં આવતી દરેક કી સ્ટ્રોકને વાંચવા માટે રચાયેલ છે. આ દૂષિત ટૂલ્સ આપણી જાણ વગર આપણા યુઝરનેમ, પાસવર્ડ, સંદેશાઓ અને અન્ય વિવિધ વ્યક્તિગત માહિતીને રેકોર્ડ કરી શકે છે. એકવાર તેઓ આ સંવેદનશીલ વિગતો એકત્રિત કરી લે પછી, આવા પ્રોગ્રામ તે માહિતી હેકર્સને મોકલે છે.

સોશિયલ એન્જિનિયરિંગ (Social Engineering)

આ હુમલાખોરો દ્વારા નકલી ઈમેઈલ, SMS, ફોન કોલ અથવા રૂબરૂ વાતચીત દ્વારા ગેરમાર્ગે દોરનારા સંદેશાવ્યવહારનો ઉપયોગ કરીને લોકોને પાસવર્ડ, બેંક વિગતો અથવા વ્યક્તિગત ડેટા જેવી સંવેદનશીલ માહિતી જાહેર કરવા માટે છેતરવાની એક પદ્ધતિ છે. કમ્પ્યૂટરને હેક કરવાને બદલે, હુમલાખોર તમારા શિક્ષક, મિત્ર અથવા બેંક અધિકારી જેવા તમે જેના પર વિશ્વાસ કરો છો તે બનવાનો ડોળ કરીને માનવમનને "હેક" કરે છે. આનો ધ્યેય તકનીકી નબળાઈઓને બદલે માનવ વિશ્વાસનો લાભ લઈને સિસ્ટમ અથવા ડેટાની ઍક્સેસ મેળવવાનો છે. ઉદાહરણ તરીકે, કોઈ અજાણી વ્યક્તિ તમારા શિક્ષક, મિત્ર અથવા સંબંધીઓ હોવાનો ડોળ કરીને તમારો લોગિન વિગતો, OTP અથવા બેંક વિગતો માંગે છે, જ્યારે તમને મદદ કરવાનો દેખાવ કરે છે. આ એક સોશિયલ એન્જિનિયરિંગ યુક્તિ છે, જેનો પછીથી દુરુપયોગ થઈ શકે છે.

ફિશિંગ (Phishing)

ફિશિંગ એ એક પ્રકારનો સોશિયલ એન્જિનિયરિંગ સાઇબર હુમલો છે જ્યાં હુમલાખોરો વિશ્વસનીય સ્રોત હોવાનો ડોળ કરીને લોકોને પાસવર્ડ, ક્રેડિટ કાર્ડ નંબર્સ અથવા OTPs જેવી વ્યક્તિગત અથવા સંવેદનશીલ માહિતી શેર કરવા માટે છેતરવાનો પ્રયાસ કરે છે. તે સામાન્ય રીતે નકલી ઈમેઈલ, સંદેશાઓ અથવા વેબસાઈટ દ્વારા થાય છે જે વાસ્તવિક લાગે છે. આ સંદેશાઓ ઘણીવાર તાકીદની ભાવના પેદા કરે છે, જેમ કે તમે ઝડપથી કાર્યવાહી નહીં કરો તો તમારું એકાઉન્ટ બ્લોક થઈ જશે.

ફિશિંગનું ઉદાહરણ :

- તમને એક ઈમેઈલ મળે છે જે તમારી બેંક તરફથી હોય તેવું લાગે છે, જે તમને એક લિંક પર ક્લિક કરવા અને તમારા એકાઉન્ટની વિગતો ચકાસવા માટે કહે છે. જો તમે ક્લિક કરો છો અને તમારી માહિતી દાખલ કરો છો, તો હુમલાખોર તેને ચોરી લે છે.

ફિશિંગ જોખમી છે કારણ કે તે ઓળખની ચોરી, નાણાકીય નુકસાન અથવા એકાઉન્ટની અનધિકૃત ઍક્સેસ તરફ દોરી શકે છે. જવાબ આપતા પહેલા હંમેશા લિંક અને મોકલનારની વિગતો ફરીવાર તપાસવી જરૂરી બને છે.

સર્વિસનો ઈનકાર (Denial of Service - DoS)

આ પ્રકારના જોખમમાં, હુમલાખોરો સિસ્ટમના સાચા વપરાશકર્તાઓ માટે તેને અનુપલબ્ધ બનાવવા માટે અતિશય ટ્રાફિક સાથે સિસ્ટમને ભરી દે છે.

ડેટા ભંગ (Data Breaches)

જ્યારે અનધિકૃત વ્યક્તિઓ ખાનગી ડેટાની ઍક્સેસ મેળવે છે અથવા તેને ખુલ્લો પાડે છે, ત્યારે ડેટા ભંગ થાય છે, જે સંભવિતપણે મહત્ત્વપૂર્ણ પ્રાઇવસીનું ઉલ્લંઘન અને નાણાકીય નુકસાન તરફ દોરી શકે છે.

મધ્યમાં રહેલો વ્યક્તિ (Man-in-the-Middle - MitM)

આ પ્રકારના હુમલાઓમાં, સંદેશાવ્યવહારમાં સામેલ કાયદેસર પક્ષોની જાણ વગર ડેટા ચોરવા માટે બે પક્ષો વચ્ચેના સંદેશાવ્યવહારને મેળવવાનો સમાવેશ થાય છે.

આંતરિક જોખમો (Insider Threats)

તેમાં એવા વ્યક્તિઓ દ્વારા કરવામાં આવતા દૂષિત કૃત્યોનો સમાવેશ થાય છે જેમની પાસે સંસ્થાની સિસ્ટમ્સનો સાચો ઍક્સેસ હોય છે, દા.ત. નાખુશ કર્મચારીઓ.

ઝીરો-ડે એક્સપ્લોઈટ (Zero-day Exploits)

ઝીરો-ડે એક્સપ્લોઈટ એ એક પ્રકારનો હુમલો છે જે પેચ (patch) અથવા ફિક્સ (fix) ઉપલબ્ધ થાય તે પહેલાં નવી શોધાયેલી વેબસાઈટ, એપ્સ અથવા ગેમની નબળાઈઓનો લાભ ઉઠાવે છે.

નકલી વેબસાઈટ્સ (Fake Websites)

વિદ્યાર્થીઓ માટે નકલી વેબસાઈટ, શંકાસ્પદ લિંક્સ અને નકલી SMS વિશે જાગૃત રહેવું મહત્ત્વપૂર્ણ છે, કારણ કે આ સાઈબર અપરાધીઓ દ્વારા વપરાશકર્તાઓને છેતરવા અને નુકસાન પહોંચાડવા માટે વપરાતી સામાન્ય યુક્તિઓ છે. નકલી વેબસાઈટ કાયદેસર સાઈટ જેવી દેખાવા માટે ડિઝાઈન કરવામાં આવે છે પરંતુ તે ખરેખર છેતરપિંડી હોય છે. આ વેબસાઈટનો હેતુ વ્યક્તિગત ડેટા ચોરવાનો અથવા તમારા ઉપકરણ પર માલવેર ઈન્સ્ટોલ કરવાનો હોય છે.

ઉદાહરણ : કલ્પના કરો કે તમને તમારી મનપસંદ ઓનલાઈન સ્ટોર તરફથી એક ઈમેઈલ મળે છે, જે ભારે

ડિસ્કાઉન્ટ ઓફર કરે છે. ઈમેઈલ તમને એક વેબસાઈટ પર નિર્દેશિત કરે છે જે વાસ્તવિક ઓનલાઈન સ્ટોર જેવી જ દેખાય છે પરંતુ તે ખરેખર તમારો લોગિન-ID અને પાસવર્ડ ચોરવા માટે રચાયેલ નકલી વેબસાઈટ છે.

સુરક્ષા ટીપ : વેબસાઈટનું સરનામું (URL) હંમેશા કાળજીપૂર્વક વાંચો. વાસ્તવિક વેબસાઈટ્સના URL "https://" અને નાના તાળાના આઈકન (padlock icon)થી શરૂ થાય છે, જે સુરક્ષિત કનેક્શન સૂચવે છે. તમને મળેલી લિંકમાં કોઈ શંકા હોય તો, તેના પર ક્લિક કરવાને બદલે તમારા બ્રાઉઝરમાં વેબસાઈટનું સરનામું સીધું ટાઈપ કરવું વધુ સુરક્ષિત છે.

શંકાસ્પદ લિંક (Suspicious Links)

શંકાસ્પદ લિંક ઘણીવાર ઈમેઈલ, સંદેશાઓ અથવા વેબસાઈટ પર જોવા મળે છે. આવી લિંક પર ક્લિક કરવાથી આપણી સિસ્ટમમાં માલવેર ડાઉનલોડ થઈ શકે છે.

ઉદાહરણ : તમને સોશિયલ મીડિયા પર કોઈ મિત્ર તરફથી "આ શાનદાર વિડિઓ જુઓ!" એમ કહીને એક લિંક સાથેનો સંદેશ મળી શકે છે. જો કે, તે લિંક તમને જોખમી સાઈટ તરફ દોરી શકે છે જે તમારા ઉપકરણને માલવેરથી સંક્રમિત કરે છે.

સુરક્ષા ટીપ : ક્લિક કરતા પહેલા તેઓ તમને ક્યાં દોરી જાય છે તે જોવા માટે વાસ્તવિક વેબસાઈટનું સરનામું વાંચવા માટે લિંક પર માઉસ ફેરવો. જો URL અજાણ્યું અથવા શંકાસ્પદ લાગે, તો તેના પર ક્લિક કરશો નહીં. મોકલનાર સાથે હંમેશા પુષ્ટિ કરો કે તેઓએ ખરેખર સંદેશ મોકલ્યો છે.

નકલી SMS (Fake SMS)

નકલી SMS, જેને સ્મિશિંગ (Smishing) તરીકે પણ ઓળખવામાં આવે છે, તે છેતરપિંડીવાળા ટેક્સ્ટ સંદેશાઓ છે જે વપરાશકર્તાઓને વ્યક્તિગત માહિતી જાહેર કરવા અથવા દૂષિત લિંક પર ક્લિક કરવા માટે છેતરવાનો પ્રયાસ કરે છે.

ઉદાહરણ : તમને એક ટેક્સ્ટ સંદેશ મળી શકે છે જેમાં કહેવામાં આવ્યું હોય કે તમે ઈનામ જીત્યા છો અને તેનો દાવો કરવા માટે એક લિંક પર ક્લિક કરવાની જરૂર છે. આ સંદેશાઓ ઘણીવાર તમારી માહિતી ચોરવા અથવા તમારા ફોન પર હાનિકારક સૉફ્ટવેર ઈન્સ્ટોલ કરવાના ઈરાદાથી કરવામાં આવતા કૌભાંડો હોય છે.

સુરક્ષા ટીપ : અજાણ્યા નંબરોમાંથી અણધાર્યા સંદેશાઓ પ્રાપ્ત થાય, ખાસ કરીને જે વ્યક્તિગત માહિતીની વિનંતી કરે અથવા તમને તાત્કાલિક પગલાં લેવા દબાણ કરે, ત્યારે કાળજીપૂર્વક વાંચો. આવા સંદેશાઓમાં આપેલી લિંક પર ક્યારેય ક્લિક કરશો નહીં, અને તેમને તાત્કાલિક ડિલીટ કરો. જો જરૂરી હોય તો, કોઈપણ પગલાં લેતા પહેલા તમારા શિક્ષક અથવા માતા-પિતાની સલાહ લો.

કમ્પ્યૂટર સુરક્ષા પદ્ધતિઓ

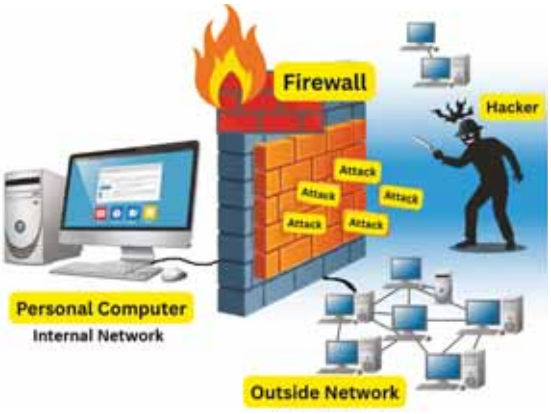
કમ્પ્યૂટર સુરક્ષા પદ્ધતિઓ વિશે સમજણ મેળવવી ઈન્ટરનેટ વપરાશકર્તાઓ માટે મહત્ત્વપૂર્ણ છે. કમ્પ્યૂટર સુરક્ષા પદ્ધતિઓ એવા ટૂલ્સ અને તકનીકો છે જે આપણા ઉપકરણો અને વ્યક્તિગત માહિતીને સાઈબર હુમલાઓથી બચાવવા માટે રચાયેલ છે. આ સુરક્ષા પદ્ધતિઓ શીખીને, આપણે આપણી ઓનલાઈન પ્રવૃત્તિઓનું રક્ષણ કરી શકીએ છીએ, અને ડિજિટલ પ્રાઈવસી અને સલામતી સુનિશ્ચિત કરી શકીએ છીએ. ચાલો કેટલીક કમ્પ્યૂટર સુરક્ષા પદ્ધતિઓને સમજીએ.

એન્ટીવાઈરસ

એન્ટીવાઈરસ એ એક કમ્પ્યૂટર પ્રોગ્રામ છે જે આપણા કમ્પ્યૂટર, મોબાઈલ ફોન અને ટેબ્લેટમાંથી વાઈરસ અને અન્ય દૂષિત પ્રોગ્રામ ને શોધવા અને દૂર કરવા માટે રચાયેલ છે. તે જોખમોને ઓળખવા અને નુકસાન પહોંચાડે તે પહેલાં તેને દૂર કરવા માટે ફાઈલ અને સિસ્ટમને નિયમિતપણે સ્કેન કરે છે. ડિજિટલ ઉપકરણોની સુરક્ષા જાળવવા માટે એન્ટીવાઈરસ સૉફ્ટવેરને અપડેટ રાખવું નિર્ણાયક છે.

ફાયરવૉલ

ફાયરવૉલ આપણા કમ્પ્યૂટર અને ઈન્ટરનેટ વચ્ચે એક અવરોધક તરીકે કાર્ય કરે છે, જે આવતા અને જતા નેટવર્ક ટ્રાફિક ને નિયંત્રિત કરે છે. ફાયરવૉલ આપણા આંતરિક ડિજિટલ સંસાધનોને હેકર્સ જેવા બહારના લોકોથી સુરક્ષિત કરે છે. તે ફક્ત માન્ય અને અસલી નેટવર્ક ટ્રાફિક ને જ આપણા આંતરિક કમ્પ્યૂટર નેટવર્કમાં પ્રવેશવાની મંજૂરી આપે છે. તે હાનિકારક ડેટાને અવરોધિત કરીને અને સુરક્ષિત ડેટાને પસાર થવા દઈને આપણી સિસ્ટમમાં અનધિકૃત પ્રવેશ અટકાવવામાં મદદ કરે છે. ફાયરવૉલ હાર્ડવેર-આધારિત, સૉફ્ટવેર-આધારિત, અથવા બંનેનું સંયોજન હોઈ શકે છે. આકૃતિ 11.2 ફાયરવોલ દર્શાવે છે.



આકૃતિ 11.2 : ફાયરવૉલ

ઈન્ટરનેટ અને Wi-Fi નો સુરક્ષિત ઉપયોગ

સુરક્ષિત ઈન્ટરનેટ કનેક્શનનો ઉપયોગ કરવો એ આપણા ડેટાને સુરક્ષિત રાખવા માટે મહત્ત્વપૂર્ણ છે. સંવેદનશીલ પ્રવૃત્તિઓ માટે સાર્વજનિક Wi-Fiનો ઉપયોગ કરવાનું ટાળો, કારણ કે આ નેટવર્ક ઘણીવાર ઓછા સુરક્ષિત હોય છે અને સાઈબર-હુમલાઓ માટે વધુ સંવેદનશીલ હોય છે. જો તમારે સાર્વજનિક Wi-Fi નો ઉપયોગ કરવો જ પડે, તો તમારા ઈન્ટરનેટ ટ્રાફિકને એન્ક્રિપ્ટ (encrypt) કરવા અને તમારી પ્રાઈવસીને સુરક્ષિત રાખવા માટે વર્ચ્યૂઅલ પ્રાઈવેટ નેટવર્ક (VPN) નો ઉપયોગ કરવાનું વિચારો.

નિયમિત સૉફ્ટવેર અપડેટ

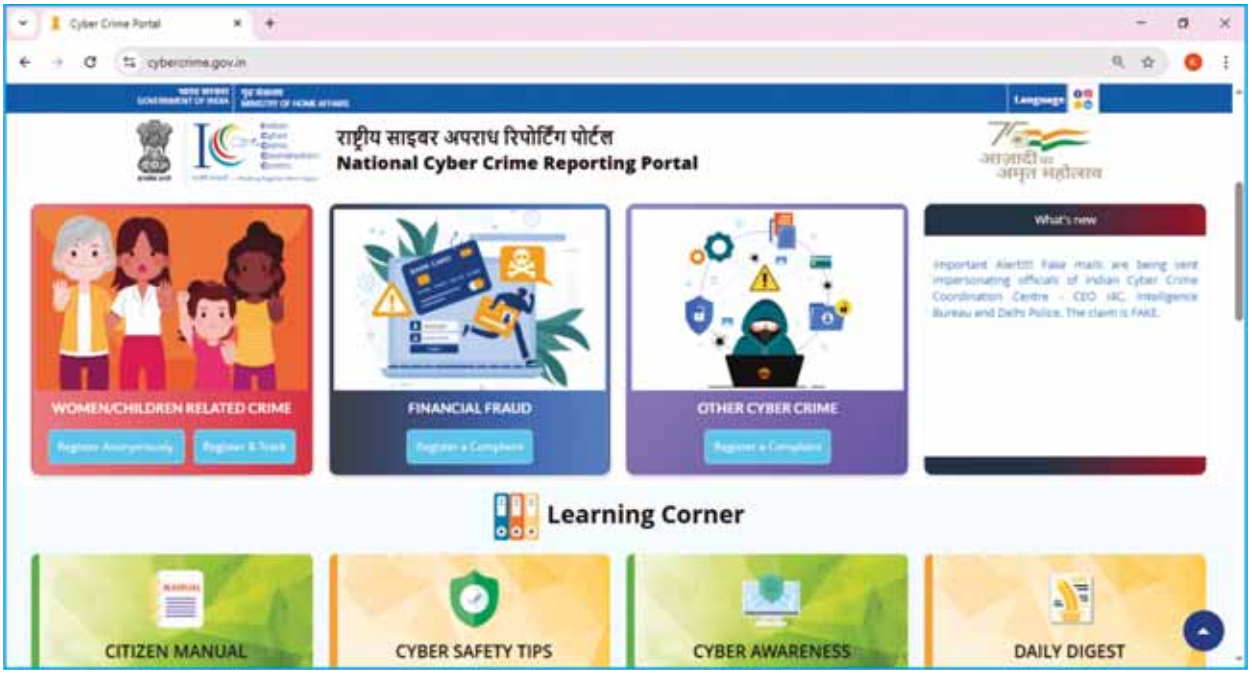
કમ્પ્યૂટર ઓપરેટિંગ સિસ્ટમ અને એપ્લિકેશનને અપ-ટુ-ડેટ રાખવી તે નબળાઈઓ અને હુમલાઓ સામે રક્ષણ આપવા માટે આવશ્યક છે. સૉફ્ટવેર અપડેટમાં ઘણીવાર સુરક્ષા પેચ (security patches) શામેલ હોય છે જે જાણીતા જોખમો અને નબળાઈઓને સંબોધિત કરે છે, જે સુનિશ્ચિત કરે છે કે તમારું ઉપકરણ નવીનતમ સાઈબર જોખમો સામે સુરક્ષિત રહે.

વપરાશકર્તાનું શિક્ષણ અને જાગૃતિ

સંભવિત સાઈબર જોખમો વિશે જાગૃત રહેવું અને તેમને કેવી રીતે ઓળખવા અને પ્રતિસાદ આપવો તેનો અભ્યાસ એ કમ્પ્યૂટર સુરક્ષાનું મુખ્ય પાસું છે. આમાં ફિશિંગ કૌભાંડો (phishing scams), નકલી વેબસાઈટ અને શંકાસ્પદ લિંક વિશે સાવચેત રહેવાનો સમાવેશ થાય છે. તમારી જાતને અને અન્ય લોકોને સલામત ઓનલાઈન પ્રથાઓ વિશે શિક્ષિત કરવાથી વધુ સુરક્ષિત ડિજિટલ વાતાવરણ બનાવવામાં મદદ મળે છે. કમ્પ્યૂટર સુરક્ષા પદ્ધતિઓને કાળજીપૂર્વક સમજીને અને અમલમાં મૂકીને વિદ્યાર્થીઓ સાઈબર જોખમોનો શિકાર બનવાનું તેમનું જોખમ નોંધપાત્ર રીતે ઘટાડી શકે છે.

ભારત સરકારનું સાઈબર ક્રાઈમ પોર્ટલ

ભારત સરકારે નેશનલ સાઈબર ક્રાઈમ રિર્પોટિંગ પોર્ટલ (National Cyber Crime Reporting Portal) નામની એક વિશેષ વેબસાઈટ શરૂ કરી છે. આ વેબસાઈટ ભારતના નાગરિકોને નાણાકીય છેતરપિંડી, સાઈબર બુલિંગ અને હેકિંગ જેવા ઓનલાઈન ગુનાઓની જાણ કરવાની મંજૂરી આપે છે. તે ઓનલાઈન સલામતી સુનિશ્ચિત કરવા અને નાગરિકોનું રક્ષણ કરવા માટેનું એક મહત્ત્વપૂર્ણ સાધન છે. આ વેબસાઈટ ઈન્ટરનેટ-સંબંધિત ગુનાઓ વિશે ફરિયાદ દાખલ કરવાનું સરળ બનાવે છે. આકૃતિ 11.3 પોર્ટલનું હોમપેજ દર્શાવે છે. (https://cybercrime.gov.in/)



આકૃતિ 11.3 : નેશનલ સાઇબર ક્રાઇમ રિર્પોટિંગ પોર્ટલ

ચાલો આ પોર્ટલ શું છે અને તેનો ઉપયોગ કેવી રીતે થઈ શકે તે વિશે વધુ જાણીએ.

તે કેવી રીતે કાર્ય કરે છે?

- **સાઇબર ક્રાઇમની જાણ કરવી :** જો તમે ઑનલાઇન કોઈ ખરાબ વસ્તુ જુઓ અથવા તેનો અનુભવ કરો, જેમ કે કૌભાંડ અથવા કોઈની સાથે ગુંડાગીરી (bullying) થઈ રહી હોય, તો તમે તેની પોર્ટલ પર જાણ કરી શકો છો. પહેલાં તમારા માતા-પિતા અથવા શિક્ષક જેવા કોઈ પુખ્ત વ્યક્તિને કહેવું મહત્ત્વપૂર્ણ છે, અને તેઓ તમને પોર્ટલનો ઉપયોગ કરવામાં મદદ કરી શકે છે.
- **ફોર્મ ભરવું :** પોર્ટલ પર એક ફોર્મ હોય છે જ્યાં તમે જે બન્યું હોય તે લખી શકો છો. તમારે વિગતો સામેલ કરવાની જરૂર પડશે જેમ કે તમને કયા પ્રકારની સમસ્યાનો સામનો કરવો પડી રહ્યો છે અને તે ક્યારે બની.
- **સુરક્ષિત રહેવું :** આ પોર્ટલ સરકારને ઑનલાઇન ખોટી પ્રવૃત્તિ કરી રહેલા લોકોને શોધવા અને તેમને રોકવામાં મદદ કરે છે. આ સમસ્યાઓની જાણ કરીને, તમે દરેક માટે ઇન્ટરનેટને સુરક્ષિત સ્થળ બનાવવામાં મદદ કરો છો.
- **મદદ મેળવવી :** એકવાર તમે સમસ્યાની જાણ કરી દો, પછી સત્તાવાળાઓ તપાસ કરી શકે છે અને સમસ્યા હલ કરવામાં મદદ કરી શકે છે. તેઓ ભવિષ્યમાં તમારી જાતને ઑનલાઇન કેવી રીતે સુરક્ષિત રાખવી તે અંગેની સલાહ પણ આપી શકે છે.

સાઇબર ક્રાઇમ પોર્ટલ મહત્ત્વપૂર્ણ છે કારણ કે તે લોકોને ઇન્ટરનેટના જોખમોથી બચાવવામાં મદદ કરે છે. સાઇબર-ક્રાઇમની જાણ કરીને, તમે ખરાબ લોકોને અન્યને નુકસાન પહોંચાડતા અટકાવવામાં મદદ કરો છો. તે દરેકને ઑનલાઇન સુરક્ષિત રહેવા વિશે પણ શીખવે છે અને આપણને જવાબદાર ડિજિટલ નાગરિકો બનવા માટે પ્રોત્સાહિત કરે છે.

યાદ રાખો ! જો તમને ક્યારેય ઑનલાઇન અસુરક્ષિત લાગે અથવા કંઈક ખોટું જણાય, તો હંમેશાં તમારાં માતા-પિતા અને તમારા વર્ગશિક્ષકને કહો. તેઓ તમને આગળ શું કરવું અને સાઇબર ક્રાઇમ પોર્ટલનો ઉપયોગ કેવી રીતે કરવો તે નક્કી કરવામાં મદદ કરી શકે છે. આ પોર્ટલ દરેક માટે ઇન્ટરનેટને સુરક્ષિત સ્થળ રાખવા માટેનું એક મહત્ત્વપૂર્ણ સાધન છે.

CERT-IN (ઇન્ડિયન કમ્પ્યૂટર ઇમરજન્સી રિસ્પોન્સ ટીમ)

CERT-IN (ઇન્ડિયન કમ્પ્યૂટર ઇમરજન્સી રિસ્પોન્સ ટીમ), એ ભારતની રાષ્ટ્રીય નોડલ એજન્સીમાંની એક છે જે જ્યારે જ્યારે કમ્પ્યૂટર સુરક્ષા ઘટનાઓ બને છે ત્યારે તેના પર પ્રતિસાદ આપવા માટે કાર્ય કરે છે. CERT-In સંસ્થાઓ અને વ્યક્તિઓને તેમની સિસ્ટમ અને નેટવર્કને સુરક્ષિત કરવામાં મદદ કરવા માટે સલાહ, સુરક્ષા ચેતવણીઓ, નબળાઈ નોંધો અને માર્ગદર્શિકાઓ જારી કરીને જોખમોનો સામનો કરે છે.

સાઈબર સુરક્ષાના જોખમો અને શ્રેષ્ઠ પ્રથાઓ પર વધુ વિગતવાર માહિતી માટે, તમે CERT-In ની સત્તાવાર વેબસાઈટની મુલાકાત લઈ શકો છો https://www.cert-in.org.in/.

નોંધ : વધારાની સાઈબર સુરક્ષા પ્રથાઓ માટે, ભારત સરકારના સત્તાવાર સાઈબર ક્રાઈમ પોર્ટલ (https://cybercrime.gov.in)ની મુલાકાત લો. નીચેની લિંક સાઈબર સુરક્ષા જાગૃતિ સુધારવા માટે મૂલ્યવાન સંસાધનો પ્રદાન કરે છે :

- સાઈબર સલામતી પર વિદ્યાર્થીઓ માટેની ખૂબ જ ઉપયોગી ડોક્યુમેન્ટ 'A handbook for students on Cyber safety' :

  https://static.cybercrime.gov.in/WebformCrime_OnlineSafetyTips.aspx

- મહત્ત્વપૂર્ણ સાઈબર જાગૃતિ દસ્તાવેજો (Cyber Awareness Documents) જુઓ :

  https://static.cybercrime.gov.in/Webform/CyberAware.aspx

સારાંશ

આ પ્રકરણમાં, વિદ્યાર્થીઓને ડિજિટલ યુગમાં કમ્પ્યૂટર સુરક્ષાનું મહત્ત્વ સમજાવવામાં આવ્યું છે, જેમાં ડિજિટલ સંસાધનો અને ડેટા પ્રાઈવસીના રક્ષણ પર ધ્યાન કેન્દ્રિત કરવામાં આવ્યું છે. તે સાઈબર સુરક્ષાના મૂળભૂત સિદ્ધાંતો, સામાન્ય સાઈબર જોખમો, મૂળભૂત કરવા યોગ્ય અને ન કરવા યોગ્ય બાબતો (do's and don'ts) અને સલામત બ્રાઉઝિંગની આદતોને આવરી લે છે. આ પ્રકરણમાં વાઈરસ, માલવેર, ફિશિંગ, રેન્સમવેર, કી લોગર્સ, સાઈબર બુલિંગ અને સોશિયલ એન્જિનિયરિંગની યુક્તિઓ જેવા વિવિધ જોખમોની ચર્ચા કરવામાં આવી છે. આ પ્રકરણ નકલી વેબસાઈટ, શંકાસ્પદ લિંક અને નકલી SMS ને કેવી રીતે ઓળખવા તે વિશે પણ જણાવે છે. તે એન્ટીવાઈરસ સૉફ્ટવેર અને ફાયરવૉલ દ્વારા ઉપકરણો અને એપ્લિકેશનના સુરક્ષિત ઉપયોગ પર ભાર મૂકતી, મહત્ત્વપૂર્ણ સુરક્ષા પદ્ધતિઓને પણ આવરી લે છે. વધુમાં, વિદ્યાર્થીઓને સાઈબર ક્રાઈમની જાણ કરવા અને તેનું નિવારણ કરવા માટેના રાષ્ટ્રીય સાઈબર ક્રાઈમ પોર્ટલ વિશે પણ માહિતી આપવામાં આવી છે, જે તેમને તેમની માહિતીને ઑનલાઈન સુરક્ષિત રાખવાની કુશળતાથી સજ્જ કરે છે.

સ્વાધ્યાય

1. કમ્પ્યૂટર સુરક્ષા શા માટે મહત્ત્વની છે?
2. શાળા દ્વારા ઉપયોગમાં લેવામાં આવતા મહત્ત્વના ડિજિટલ સંસાધનોની યાદી બનાવો.
3. ડેટા પ્રાઈવસી એટલે શું?
4. મજબૂત પાસવર્ડ કેવી રીતે બનાવી શકાય છે? મજબૂત પાસવર્ડના કોઈપણ ત્રણ ઉદાહરણ આપો.
5. નબળો પાસવર્ડ એટલે શું? ત્રણ નબળા પાસવર્ડનાં ઉદાહરણ આપો.
6. ઈન્ટરનેટનો ઉપયોગ કરતી વખતે વિદ્યાર્થીએ સલામત બ્રાઉઝિંગ માટે ધ્યાનમાં રાખવાના ત્રણ મુદ્દા જણાવો.
7. સામાન્ય રીતે ઉદ્ભવતાં સાઈબર જોખમોની યાદી બનાવો.
8. રેન્સમવેર એટલે શું?
9. મોબાઈલ એપ ડાઉનલોડ કરતી વખતે સલામતી અંગે ધ્યાનમાં રાખવાના મુદ્દાઓ કયા છે?
10. Wi-Fiના સુરક્ષિત ઉપયોગ અને જાહેર Wi-Fiનો ઉપયોગ કરવામાં રહેલા જોખમો અંગે ટૂંકમાં નોંધ લખો.

11. સાચું કે ખોટું જણાવો.

(1) એન્ટીવાઈરસથી નિયમિત સ્કેન કરવામાં આવે તો માલવેર, વાઈરસ અને અન્ય સાઈબર જોખમોથી બચી શકાય છે.

(2) ફાયરવૉલ તમારા કમ્પ્યૂટર અને ઈન્ટરનેટ પર રહેલા જોખમો વચ્ચે અવરોધ તરીકે કાર્ય કરે છે.

(3) જુદાજુદા સોશિયલ મીડિયા એકાઉન્ટ પર એકસરખો પાસવર્ડ રાખવો સલામત છે.

(4) ઝીરો ડે એક્સપ્લોઈટ દ્વારા બે પક્ષો વચ્ચે થતા સંચારણમાંથી કાયદેસર ઉપયોગકર્તાની જાણ બહાર ડેટા ચોરવામાં આવે છે.

(5) ટ્રોજન એક એવો દૂષિત કોડ છે જે તમારા લોક કરેલ ડેટા પાછો મેળવવા માટે પૈસાની માગણી કરે છે.

12. ખાલી જગ્યા પૂરો.

(1) તમારા સૉફ્ટવેરને નિયમિત _____ કરવા તેનો મૂળભૂત કરવાલાયક કાર્યમાં સમાવેશ થાય છે.

(2) _____ એટલે એવી શ્રેણીના લોકો જે કમ્પ્યૂટર સિસ્ટમની નબળાઈનો દુરુપયોગ કરીને અનધિકૃત એક્સેસ અને વિગતોનો દુરુપયોગ કરે છે.

(3) અક્ષરો, અંકો અને વિશિષ્ટ અક્ષરોના સમૂહથી બનાવેલા પાસવર્ડને _____ પાસવર્ડ કહે છે.

(4) એન્ટીવાઈરસનો ઉપયોગ સાધનને _____ થી સુરક્ષિત બનાવે છે.

(5) સાઈબર ક્રાઈમ પોર્ટલ ઓફ ગવર્નમેન્ટ ઓફ ઈન્ડિયાની વેબસાઈટ પર _____ પ્રવૃત્તિની ફરિયાદ કરી શકાય છે.

13. બહુવિકલ્પી પ્રશ્નો. સૌથી યોગ્ય વિકલ્પ પસંદ કરો.

(1) સાઈબર સુરક્ષાનો પ્રાથમિક ઉદ્દેશ શું છે?

(a) કમ્પ્યૂટરની ઝડપ વધારવી (b) ડિજિટલ ડેટાને અનધિકૃત એક્સેસથી સુરક્ષા આપવી

(c) ઈન્ટરનેટ બેન્ડવિડ્થ વધારવી (d) ગ્રાફિકની ગુણવત્તા સુધારવી

(2) સુરક્ષિત બ્રાઉઝિંગ ટેવ અનુસરવી શા માટે મહત્ત્વનું છે?

(a) તમારા ઈન્ટરનેટ કનેક્શનને ઝડપી બનાવવું

(b) સાઈબર જોખમોના સંપર્કમાં આવવાથી બચવા અને વ્યક્તિગત માહિતીનું રક્ષણ કરવા માટે

(c) વધુ વેબસાઈટની મુલાકાત લેવી

(d) કમ્પ્યૂટર ગ્રાફિક સુધારવા

(3) નીચેનામાંથી કયું સાઈબર જોખમ કાયદેસર સૉફ્ટવેર જેવું લાગે છે, પરંતુ એકવાર સક્રિય થયા પછી, હાનિકારક ક્રિયાઓ કરે છે?

(a) વાઈરસ (b) વૉર્મ (c) ટ્રોજન (d) રેન્સમવેર

(4) ડેટાને અનલૉક કરવા માટે ચુકવણીની માંગણી કરતી જોખમોની શ્રેણી કઈ છે?

(a) રેન્સમવેર (b) વાઈરસ (c) ટ્રોજન (d) એડવેર

(5) નીચેનામાંથી કઈ સાઈબર સુરક્ષા માટે ભલામણ કરેલ ''કરવા યોગ્ય (do)'' બાબત છે?

(a) બધા એકાઉન્ટ માટે સમાન પાસવર્ડનો ઉપયોગ કરવો

(b) વારંવાર પોપ-અપ જાહેરાતો પર ક્લિક કરવું

(c) તમારા સૉફ્ટવેરને નિયમિતપણે અપડેટ કરવું

(d) મિત્રો સાથે પાસવર્ડ શેર કરવો

(6) મૂળભૂત સાઈબર સુરક્ષા પ્રથાઓમાં ''ન કરવા યોગ્ય (don't)'' શું છે?

(a) મજબૂત, અનન્ય પાસવર્ડનો ઉપયોગ કરવો

(b) અસુરક્ષિત વેબસાઈટ પર વ્યક્તિગત ડેટા શેર કરવો

(c) સાર્વજનિક કમ્પ્યૂટરમાંથી લોગ આઉટ કરવું

(d) ટુ-ફેક્ટર ઓથેન્ટિકેશન ચાલુ કરવું

(7) સાઇબર બુલિંગમાં સામાન્ય રીતે શાનો સમાવેશ થાય છે?

(a) શારીરિક નુકસાન (b) કોઈને હેરાન કરવા માટે ટેક્નોલોજીનો ઉપયોગ કરવો

(c) કાનૂની કાર્યવાહી (d) શૈક્ષણિક અપ્રમાણિકતા

(8) પબ્લિક Wi-Fi નેટવર્કનો ઉપયોગ કરવો શા માટે જોખમી છે?

(a) હેકર આપણો ડેટા ચોરી શકે છે.

(b) આવી લિંક પર ક્લિક કરવું સલામત છે.

(c) તેને પાસવર્ડની જરૂર પડે છે

(d) તે વધુ મોંઘું છે

(9) નીચેનામાંથી કયું શંકાસ્પદ લિંક સાથે સંબંધિત છે?

(a) તેમાં સ્પષ્ટ અને વાંચી શકાય તેવું URL હોય છે

(b) તે વિશ્વસનીય સ્રોત પરથી આવેલી જણાય છે.

(c) તેની વારંવાર મુલાકાત લેવાય છે

(d) આવી લિંક્સ પર ક્લિક કરવાથી માલવેર ડાઉનલોડ થાય છે

(10) નીચેનામાંથી કયો માલવેરનો એક પ્રકાર છે?

(a) ફાયરવૉલ (b) વાઇરસ (c) એન્ક્રિપ્શન (d) બ્રાઉઝર

પ્રાયોગિક સ્વાધ્યાય

1. *https://cybercrime.gov.in* વેબસાઇટની મુલાકાત લો અને *Learning Corner* વિભાગ હેઠળ આપેલી વિવિધ સાઇબર સલામતી માર્ગદર્શિકાઓ શોધો. તેમાંથી કોઈ એક સાઇબર સલામતી માર્ગદર્શિકા પર સંક્ષિપ્ત નોંધ લખો.
2. CERT-In ની સત્તાવાર વેબસાઇટ *https://www.cert-in.org.in/* ની મુલાકાત લો અને વેબસાઇટ પર ઉલ્લેખિત નવીનતમ *સુરક્ષા ચેતવણીઓ (Security Alerts)* માંથી કોઈપણ ત્રણ પર સંક્ષિપ્ત નોંધ તૈયાર કરો.
3. કોઈપણ પાંચ લોકપ્રિય એન્ટીવાઇરસ સૉફ્ટવેરની યાદી તૈયાર કરો.
4. કોઈપણ પાંચ નમૂનારૂપ નબળા પાસવર્ડની યાદી તૈયાર કરો. તેઓને નબળા પાસવર્ડ્સ શા માટે કહેવામાં આવે છે તેનું કારણ લખો.
5. કોઈપણ પાંચ મજબૂત પાસવર્ડ બનાવો, અને તેઓને મજબૂત પાસવર્ડ શા માટે કહેવામાં આવે છે તેનું કારણ લખો. (નોંધ : તમારા જવાબમાં તમારા વાસ્તવિક પાસવર્ડ લખશો નહીં.)
6. વિવિધ URLs ની મુલાકાત લો અને સુરક્ષિત વેબસાઇટને ઓળખો. ત્રણ સુરક્ષિત વેબસાઇટ્સની યાદી બનાવો.
   - હિન્ટ : વેબસાઇટના નામમાં *https://* ને જુઓ.
7. તમારા કમ્પ્યૂટર માટે એક સુરક્ષા ચેકલિસ્ટ તૈયાર કરો:
   - કાર્ય : ખાતરી કરવા માટે ચકાસો કે એન્ટીવાઇરસ સૉફ્ટવેર ઇન્સ્ટોલ કરેલ છે, ઓપરેટિંગ સિસ્ટમ અપડેટ થયેલ છે, અને સ્ક્રીન લોકસક્ષમ છે, વગેરે.
8. એક "સાઇબર સલામતી પોસ્ટર" બનાવો.
   - હિન્ટ : પાંચ સલામતી નિયમોનો સમાવેશ કરો (દા.ત., OTP શેર ન કરો, પાસવર્ડ શેર ન કરો, વગેરે).
9. "વિદ્યાર્થીઓ માટે સલામત બ્રાઉઝિંગની આદતો" પર એક પોસ્ટર તૈયાર કરો.
10. "સામાન્ય સાઇબર જોખમો અને તેના નિવારણની પદ્ધતિઓ" પર એક પોસ્ટર તૈયાર કરો.