14 ઇન્ટરનેટ, ઇ-મેઇલ અને સલામતી

ઇન્ટરનેટ શું છે અને તેના ઉપયોગ માટે વેબબ્રાઉઝરને કેવી રીતે અસરકારક રીતે ઉપયોગમાં લઈ શકાય, તે આપણે અગાઉના પ્રકરણમાં ચર્ચા કરી. અહીં હવે આપણે ઇલેક્ટ્રૉનિક મેઇલ (Electronic mail) વિશે ચર્ચા કરીશું. ઇ-મેઇલના ટૂંકા નામથી ઓળખાતા ઇલેક્ટ્રૉનિક મેઇલ આજકાલ સંચારણ માટે અનિવાર્ય માધ્યમ બની ગયા છે. શરૂઆતમાં તેનો ઉપયોગ એક કમ્પ્યૂટરથી બીજા કમ્પ્યૂટર સુધી માત્ર લખાણ પ્રકારના સંદેશાઓ મોકલવા માટે કરવામાં આવતો. ત્યાર બાદ આજ સુધી ઇ-મેઇલનો ઉત્તરોત્તર વિકાસ થતો રહ્યો છે. આજે ઇ-મેઇલનો ઉપયોગ માત્ર લખાણ મોકલવા માટે જ મર્યાદિત રહ્યો નથી. હવે ચિત્ર, ધ્વનિ, દસ્તાવેજ, પ્રોગ્રામ કે ઍનિમેટેડ મૂવી પણ ઇ-મેઇલ સાથે મોકલી શકાય છે. ઇ-મેઇલની કાર્યપદ્ધતિ, તેના ફાયદા અને ગેરફાયદા વિશે આપણે આ પ્રકરણમાં માહિતી મેળવીશું. તદુપરાંત ઇન્ટરનેટની સુરક્ષા માટેના સલામતી વિકલ્પો અંગે પણ જાણકારી મેળવીશું.

ઇ-મેઇલ (E-mail) :

કમ્પ્યૂટર નેટવર્ક વચ્ચે ઇલેક્ટ્રૉનિક માધ્યમથી કરવામાં આવતા સંદેશા-પ્રત્યાયનને ઇ-મેઇલ કહે છે. માટે જ તેને ઇલેક્ટ્રૉનિક મેઇલ તરીકે ઓળખવામાં આવે છે. ઇ-મેઇલ એક એવી પદ્ધતિ છે, જેમાં ઇન્ટરનેટનો ઉપયોગ કરી પ્રેષક એક કે અનેક પ્રાપ્તકર્તાઓની સાથે ડિજિટલ સંદેશાઓની આપ-લે કરી શકે છે.

પ્રાચલ	પરંપરાગત ટપાલ	ઇ-મેઇલ
સરનામું	14, સ્ટારકૉલોની, રામપુર	sweety@yahoo.com
સમય	બેથી ત્રણ દિવસ	તાત્કાલિક, સેકન્ડ કે મિનિટોમાં
વિગત	કોઈ પણ વસ્તુ પાર્સલ સ્વરૂપે મોકલી શકાય.	ઍડ્રેસબુક, ટેમ્પલેટ અને તૈયાર ડ્રાફ્ટ-સંદેશાઓ. મલ્ટિમીડિયા માહિતી પણ મોકલી શકાય.
ખર્ચ	મોકલવાનો ખર્ચ, ટિકિટો, કાગળ અને પરબીડિયાનો ખર્ચ તથા મોટાં પાર્સલ માટે પરિવહન ખર્ચ	ઇન્ટરનેટની સુવિધા ધરાવતું કમ્પ્યૂટર હોય, તો નિ:શુલ્ક
ક્યાંથી ઉપયોગમાં લઈ શકાય ?	મર્યાદિત સ્થળો પરથી ઉપયોગમાં લઈ શકાય.	કોઈ પણ સ્થળેથી ઉપયોગમાં લઈ શકાય.

કોષ્ટક 14.1 : પરંપરાગત ટપાલ વિ. ઇ-મેઇલ

ઇન્ટરનેટ પર સૌથી વ્યાપક પ્રમાણમાં ઉપયોગમાં લેવામાં આવતી સેવા ઈ-મેઇલ છે. શરૂઆતમાં ઈ-મેઇલનો ઉપયોગ માત્ર શાબ્દિક સંદેશા મોકલવા માટે કરવામાં આવતો. વર્તમાન સમયમાં તેના દ્વારા ઑડિયો, વીડિયો, ઍનિમેશન, આલેખો અને લખાણ જેવી વિવિધ પ્રકારની માહિતી પણ મોકલી શકાય છે. આ પ્રકારની માહિતીને સંયુક્તપણે મલ્ટિમીડિયા માહિતી કહે છે. કમ્પ્યૂટર નેટવર્કનો ઉપયોગ કરીને ડિજિટલ મલ્ટિમીડિયા સંદેશાઓને દુનિયાના કોઈ પણ સ્થળે ત્વરિત પ્રસારિત કરવા એ ઈ-મેઇલ પદ્ધતિનો મુખ્ય ફાયદો છે. પરંપરાગત ટપાલ સેવાની તુલનામાં ઈ-મેઇલ સેવા ઝડપી અને સસ્તી છે. પરંપરાગત ટપાલસેવા કરતા ઈ-મેઇલ એટલી વધુ અસરકારક સેવા છે કે લોકો પરંપરાગત ટપાલને સ્નેઇલ મેઇલ (Snail mail) તરીકે ઓળખવા લાગ્યા છે. કોષ્ટક 14.1માં આ રૂપરેખા જોવા મળશે, જેમાં ધીમી ગતિ (સ્નેઇલ) ટપાલસેવાની ઈ-મેઇલ સાથે તુલના દર્શાવી છે.

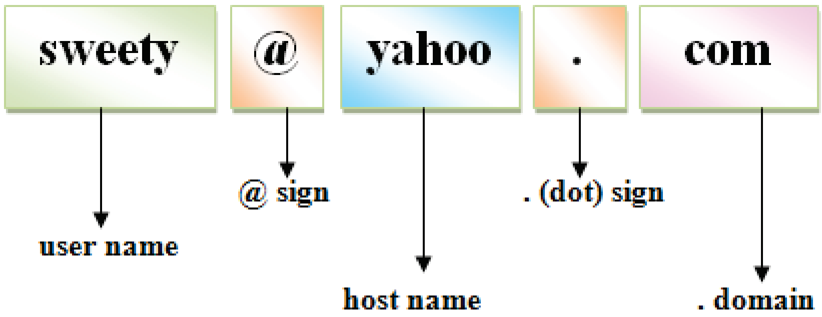
વ્યાવસાયિક સંચરણ વધુ સારી રીતે કરવા, માહિતીનો વધુ અસરકારક ઉપયોગ કરવા તથા સમય અને ખર્ચનો બચાવ કરવા ઈ-મેઇલ ઉપયોગી સેવા છે. ઈ-મેઇલ દ્વારા મળતા લાભ કોષ્ટક 14.2માં દર્શાવ્યા છે :

તે ત્વરિત છે.	મોટા ભાગના સંદેશાઓ અમુક સેકન્ડ કે મિનિટો જેવા ઓછા સમયમાં પહોંચાડી શકાય છે.
તે વૈશ્વિક છે.	કોઈ જ ભૌગોલિક મર્યાદા વગર આખી દુનિયામાં કોઈ પણ સ્થળે સંદેશ મોકલી શકાય છે. ઉપરાંત, ઈ-મેઇલ સેવાનો ઉપયોગ વિવિધ પ્રકારનાં સાધનો (મોબાઇલ કે iPod) દ્વારા પણ કરી શકાય છે.
તે કરકસરયુક્ત છે.	Gmail, hotmail અને yahoo જેવી અનેક સંસ્થાઓ ઈ-મેઇલની સેવા પૂરી પાડે છે. આ સેવા નિ:શુલ્ક છે. આ માટે માત્ર ઇન્ટરનેટની સુવિધા ધરાવતું કમ્પ્યૂટર પર્યાપ્ત છે.
તે અંગત છે.	ટેલિફોનની જેમ વૈયક્તિક સંદેશાઓ ઈ-મેઇલ દ્વારા મોકલી શકાય છે.
તે વધુ સુવિધાયુક્ત છે.	ઈ-મેઇલ સેવા કૅલેન્ડર, ઍડ્રેસબુક તથા અનુકૂળ, ઉત્પાદક અને ત્વરિત સંદેશાઓ માટેના ટેમ્પલેટ સાથે ઉપલબ્ધ બને છે.
તે વિગતો સુધારવાની અનુમતિ આપે છે.	સંદેશ મોકલતા પહેલાં તેની જોડણી, વ્યાકરણ વગેરે ચકાસી અને સુધારી શકાય છે.
તે સંચરણ અંગેના દસ્તાવેજ પૂરા પાડે છે.	પ્રેષિત સંદેશા તથા સ્વીકૃત સંદેશાઓને ભવિષ્યના ઉપયોગ માટે કમ્પ્યૂટરમાં સંગ્રહી શકાય છે તથા મુદ્રિત પણ કરી શકાય છે.
એક જ સમયે અનેક વ્યક્તિઓ સુધી પહોંચવું	કોઈ પણ સંદેશ એક જ સમયે એક કે અનેક વ્યક્તિઓને પહોંચાડી શકાય છે.
તે અનેક વેબસેવા માટે પ્રવેશદ્વાર પૂરું પાડે છે.	ફેસબુક અને ટ્વીટર જેવી જુદી-જુદી સોશિયલ નેટવર્કિંગની સાઇટ પર ઈ-મેઇલ સરનામાનો ઉપયોગ કરી પ્રવેશ મેળવી શકાય છે. આ ઉપરાંત ઇન્ટરનેટ પરની અન્ય કેટલીક સેવાઓ ઉપલબ્ધ કરવા માટે ઈ-મેઇલ સરનામાનો ઉપયોગ કરવામાં આવે છે.

કોષ્ટક 14.2 : ઈ-મેઇલના ફાયદા

ઈ-મેઇલ સુવિધાના કેટલાક ગેરફાયદા અને મર્યાદાઓ પણ છે. સૌપ્રથમ તો આ સેવા માટે કમ્પ્યૂટર અને ઇન્ટરનેટ સુવિધા જરૂરી છે. વળી, ઉપયોગકર્તાને જન્કમેઇલ (junk mail) કે સ્પામમેઇલ (spam mail) તરીકે ઓળખાતા બિનજરૂરી સંદેશાઓ મોકલવામાં આવી શકે છે. કેટલીક બિનજરૂરી જાહેરાતો, નકલી પરિસંવાદ માટેનાં આમંત્રણ, અજાણી વ્યક્તિ દ્વારા માંગવામાં આવતી મદદ અથવા તો કમ્પ્યૂટરને કે તેમાં રહેલી વિગતનો નુકસાન પહોંચાડે તેવા પ્રોગ્રામ (virus) આનાં ઉદાહરણ છે.

ઈ-મેઇલ સુવિધાનો ઉપયોગ કરતાં પહેલાં કેટલીક મૂળભૂત જરૂરિયાતો પરિપૂર્ણ કરવી જરૂરી બને છે. અગાઉ જણાવવામાં આવ્યું છે તેમ પ્રેષક અને પ્રાપ્તકર્તા બંનેનાં કમ્પ્યૂટર પાસે ઇન્ટરનેટની સેવા અને ઈ-મેઇલ સરનામાં હોવાં જરૂરી છે. જો સંદેશો મેળવનાર વ્યક્તિ તે સમયે કમ્પ્યૂટર સાથે કાર્ય કરતી ન હોય, તો જ્યારે તે કમ્પ્યૂટર શરૂ કરી ઇન્ટરનેટ સાથેનું જોડાણ કરે છે, ત્યારે મેળવવામાં આવેલ સંદેશા તેના મેઇલબૉક્સમાં જોવા મળે છે. નીચે આપેલ આકૃતિ 14.1માં નમૂનારૂપ ઈ-મેઇલ સરનામું *sweety@yahoo.com* દર્શાવ્યું છે.



આકૃતિ 14.1 : ઈ-મેઇલ સરનામું અને તેના ઘટકો

ઈ-મેઇલ સરનામાની શરૂઆત ઉપયોગકર્તાએ પસંદ કરેલ નામ (યૂઝરનેમ)થી થાય છે. ઉપયોગકર્તા પોતાને પસંદ હોય તેવું કોઈ પણ નામ યૂઝરનેમ તરીકે રાખી શકે છે. માત્ર એટલું ધ્યાન રાખવું જરૂરી છે કે તે નામ તે ઈ-મેઇલ સેવા આપનારને ત્યાં અન્ય કોઈ ઉપયોગકર્તાને ફાળવવામાં આવેલું ન હોય. ઉદાહરણ તરીકે, sweety ઘણું પ્રચલિત નામ છે. જો તે નામની નોંધણી પહેલેથી થયેલી હોય, તો તેમાં થોડો ફેરફાર કરી sweety_97 જેવું બીજું કોઈ નામ પસંદ કરી શકાય છે. આમ કરવાથી ઈ-મેઇલ સરનામું sweety_97@yahoo.com બનશે. યૂઝરનેમ પછી '@' નિશાની મૂકવામાં આવે છે, જે યૂઝરનેમને ઈ-મેઇલના અન્ય ભાગથી છૂટું પાડે છે. આ નિશાની મૂક્યા પછી ઈ-મેઇલ સેવા આપનાર સંસ્થાનું નામ (જેને હોસ્ટ નેમ પણ કહે છે) મૂકવામાં આવે છે. ઉપર દર્શાવેલ સરનામામાં 'yahoo' હોસ્ટનેમ છે. ઈ-મેઇલ સરનામું વધુમાં વધુ 255 અક્ષરોનું હોઈ શકે છે તથા તેમાં લોઅરકેસ અક્ષરો a થી z, અંકો તથા ".", "_" અને "-" (પૂર્ણવિરામ, અન્ડરસ્કોર અને હાઇફન) સમાવી શકાય છે. ઈ-મેઇલ ઍડ્રેસમાં દશાંશચિહ્ન પછી ડોમેઇન નેમ લખવામાં આવે છે. આપણે આગળના પ્રકરણમાં જોઈ ગયા તે મુજબ અનેક પ્રકારનાં ડોમેઇન નામ ઉપલબ્ધ છે. એનો અર્થ એવો થયો કે આપણી પાસે sweety@yahoo.co.in કે sweety@glsict.org કે sweety@glsict.ac.in જેવાં ઈ-મેઇલ સરનામાં હોઈ શકે છે.

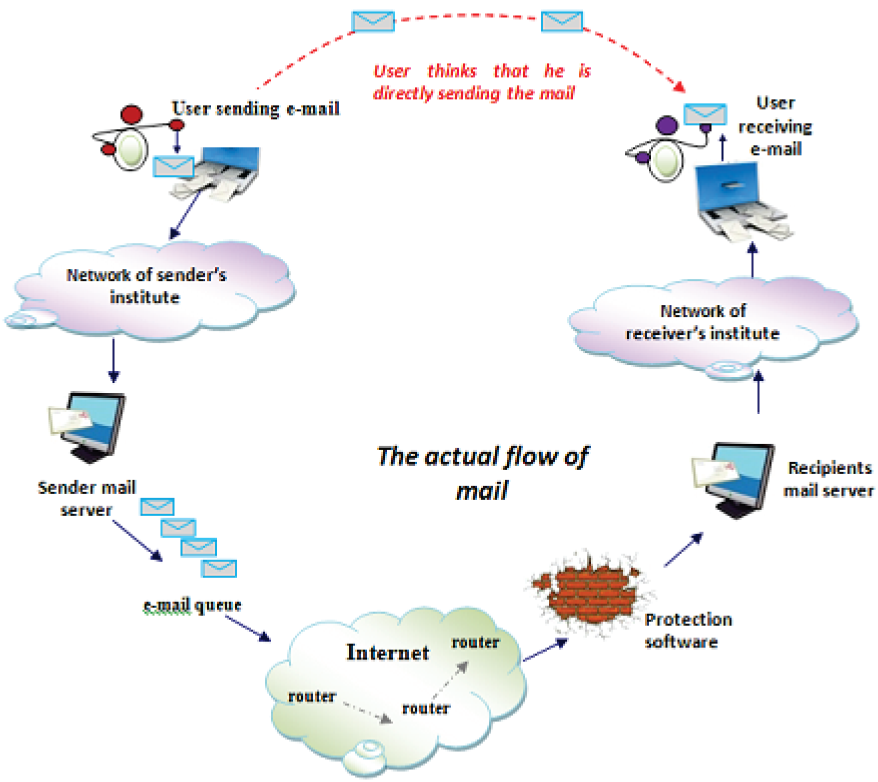
ઈ-મેઇલનું માળખું (Structure of E-mail) :

જો ઇન્ટરનેટની સેવા ઉપલબ્ધ હોય, તો ઈ-મેઇલ માટે yahoo, hotmail, gmail, indiatimes, rediffmail, વગેરે જેવી સંસ્થાઓનો ઈ-મેઇલની સેવા માટે સંપર્ક કરી શકાય છે તથા યૂઝરનેમ (અને પાસવર્ડ) પસંદ કરી તેના પર નવા ઈ-મેઇલ સરનામાની નોંધણી કરાવી શકાય છે. નોંધણી (registration) પ્રક્રિયાને ઘણીવાર 'sign up' પ્રક્રિયા પણ કહે

છે. સાઈન-અપ પ્રક્રિયા માત્ર એક જ વાર કરવાની હોય છે. ત્યાર પછી જ્યારે જ્યારે ઈ-મેઈલનો ઉપયોગ કરવા માંગતા હોઈએ ત્યારે 'sign in' કરવાની જરૂર પડે છે. નમૂનારૂપ ઈ-મેઈલના મૂળભૂત ભાગોમાં 'હેડર' આવેલું હોય છે. જેમાં પ્રેષકનું સરનામું, પ્રાપ્તકર્તાનું સરનામું, સંદેશાનો વિષય, બિડાણ અને સંદેશાનો સમાવેશ કરવામાં આવે છે. ઈ-મેઈલ અંગેનાં નમૂનારૂપ કાર્યોમાં સંદેશ મોકલવો (send), સંદેશ લખવો (compose), સંદેશનો પ્રત્યુત્તર આપવો (reply) અને એક સ્થાનેથી આવેલ સંદેશાને અન્ય સ્થાને મોકલવો (forward) જેવી ક્રિયાઓનો સમાવેશ કરી શકાય. વૈકલ્પિક રીતે, ઈ-મેઈલ સંદેશા સાથે મર્યાદિત કદ ધરાવતી ફાઈલનું બિડાણ કરી શકાય છે. આ પ્રકારની ફાઈલો દસ્તાવેજો, સંગીત અને ચિત્ર ધરાવતી મલ્ટિમીડિયા ફાઈલ હોઈ શકે છે.

ઈ-મેઈલની કાર્યપદ્ધતિ (Working of E–mail) :

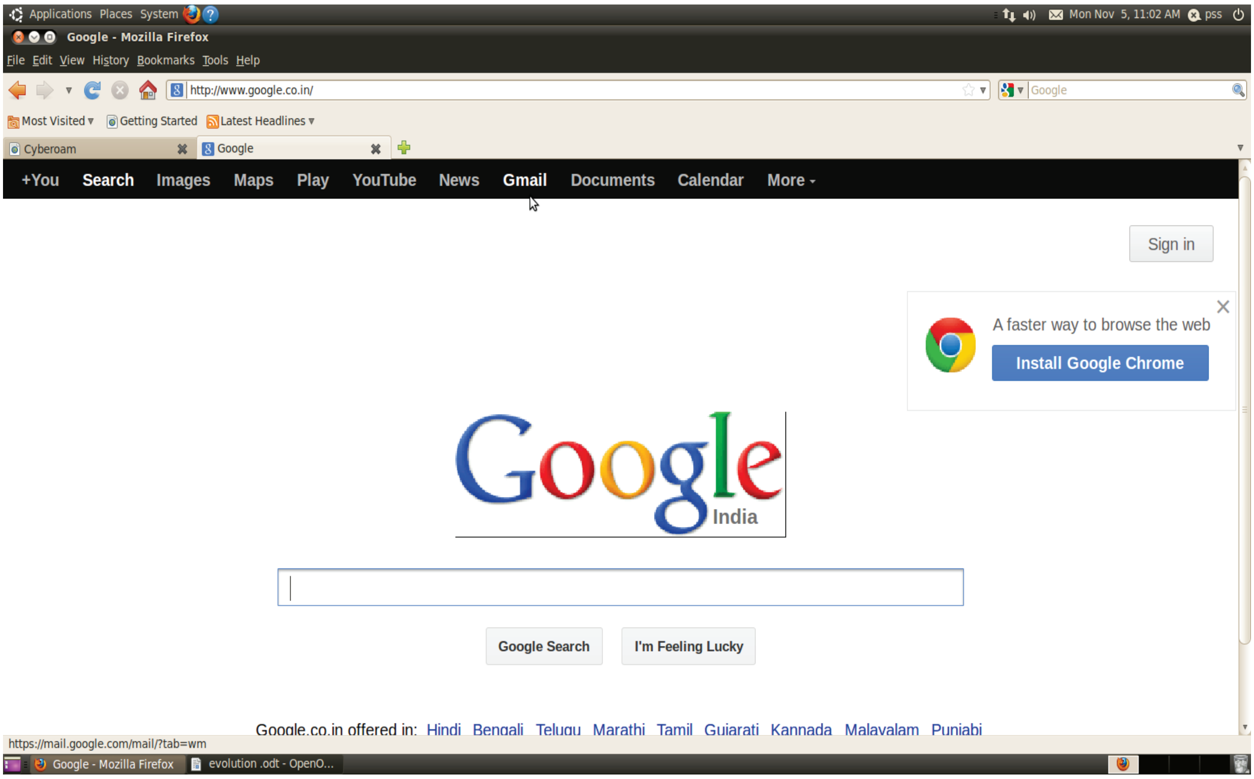
ઈ-મેઈલ સંદેશો મોકલવામાં આવે છે ત્યારે તે પ્રથમ પ્રેષકના નેટવર્કમાં જાય છે અને ત્યાર બાદ તે ઈન્ટરનેટના માધ્યમ દ્વારા પ્રાપ્તકર્તાના નેટવર્ક સુધી પહોંચે છે. અને રાઉટરની મદદથી યોગ્ય માર્ગ શોધી સર્વર સુધી પહોંચે છે. આ પ્રક્રિયા બાદ તેને ફાયરવૉલ કે તેના જેવા અન્ય સુરક્ષાના સ્તરોમાંથી પસાર થવું પડે છે. ફાયરવૉલમાંથી પસાર થતી વખતે ઈ-મેઈલને સ્પામ (બિનજરૂરી સંદેશા) તથા વાઈરસથી સુરક્ષા માટે ચકાસવામાં આવે છે. પ્રાપ્તકર્તાના નેટવર્ક પરથી તેને પ્રાપ્તકર્તાના કમ્પ્યૂટર સુધી પહોંચાડવામાં આવે છે. ઈ-મેઈલ અનુસરી શકે તેવા અભિગમાત્મક માર્ગને આકૃતિ 14.2 માં દર્શાવ્યો છે.



આકૃતિ 14.2 : ઈ-મેઈલની કાર્યપદ્ધતિ

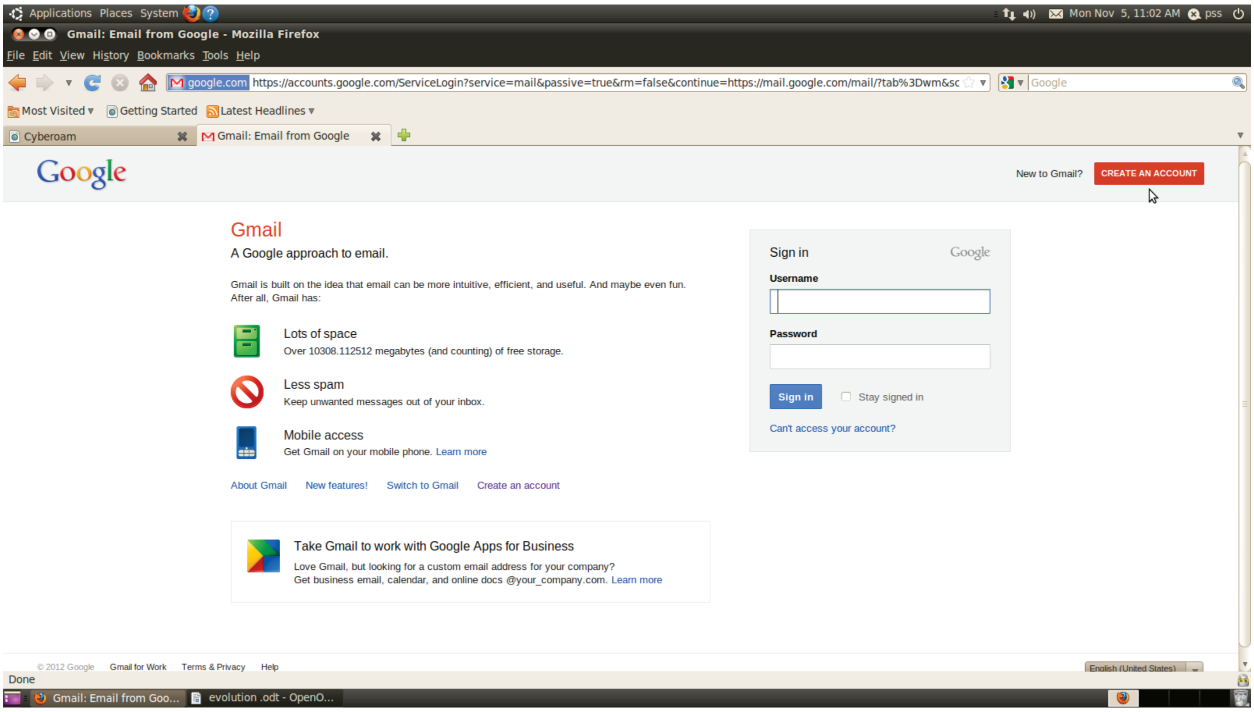
ઈ-મેઈલ એકાઉન્ટની રચના કરવી (Creating an E-mail Account) :

વર્તમાન યુગમાં વયસ્કથી લઈને વરિષ્ઠ વય સુધીની દરેક વ્યક્તિ પોતાનું ઈ-મેઈલ એકાઉન્ટ ધરાવતી નજરે પડે છે. આપણે પણ Gmailની મદદથી ઈ-મેઈલ એકાઉન્ટ બનાવવાનો પ્રયત્ન કરીએ. Googleમાં મેઈલ એકાઉન્ટની રચના કરવા માટે નીચે જણાવેલાં પગલાં અનુસરવા જરૂરી છે. Googleની વેબસાઈટ પર જઈ આકૃતિ 14.3માં દર્શાવ્યા મુજબ Gmail લિંક પર ક્લિક આપો.



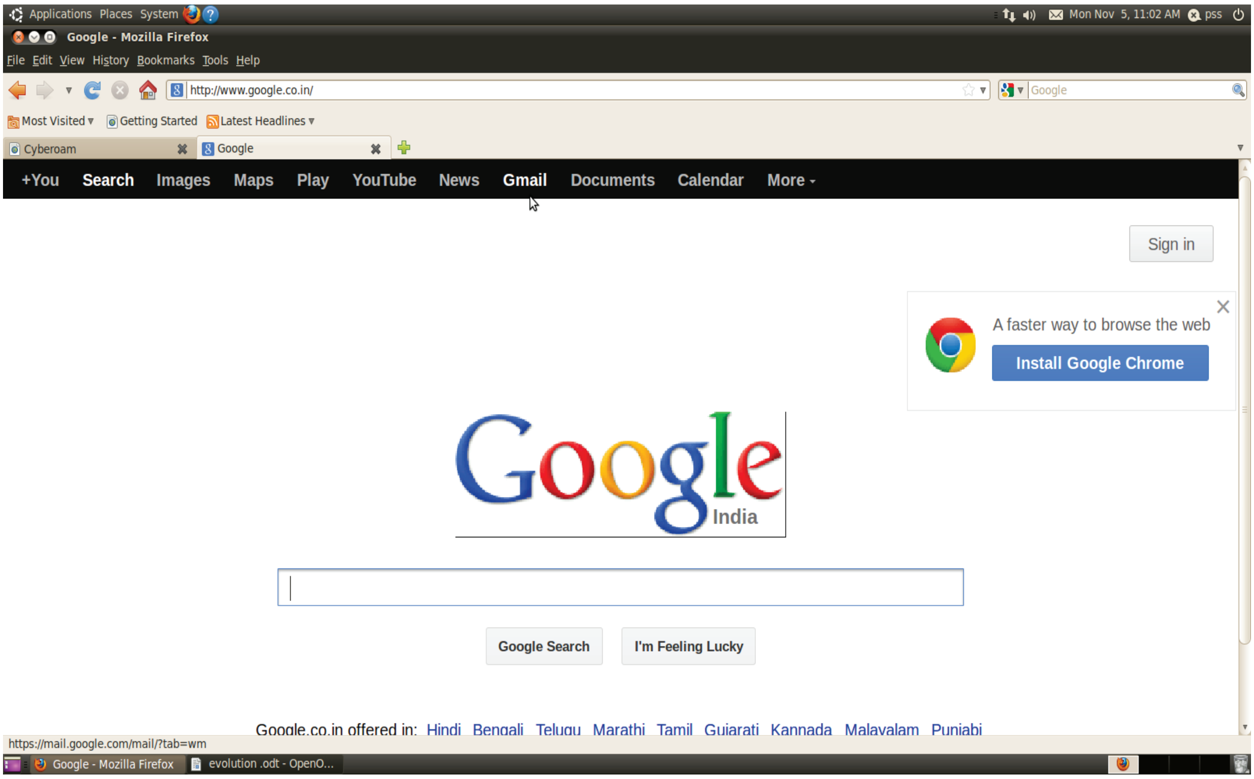
આકૃતિ 14.3 : ઈ-મેઈલ એકાઉન્ટ બનાવવા માટે Gmail પસંદ કરવું

આકૃતિ 14.4માં દર્શાવ્યા પ્રમાણેનું દૃશ્ય જોવા મળશે. અહીં Create New Account પર ક્લિક આપો.



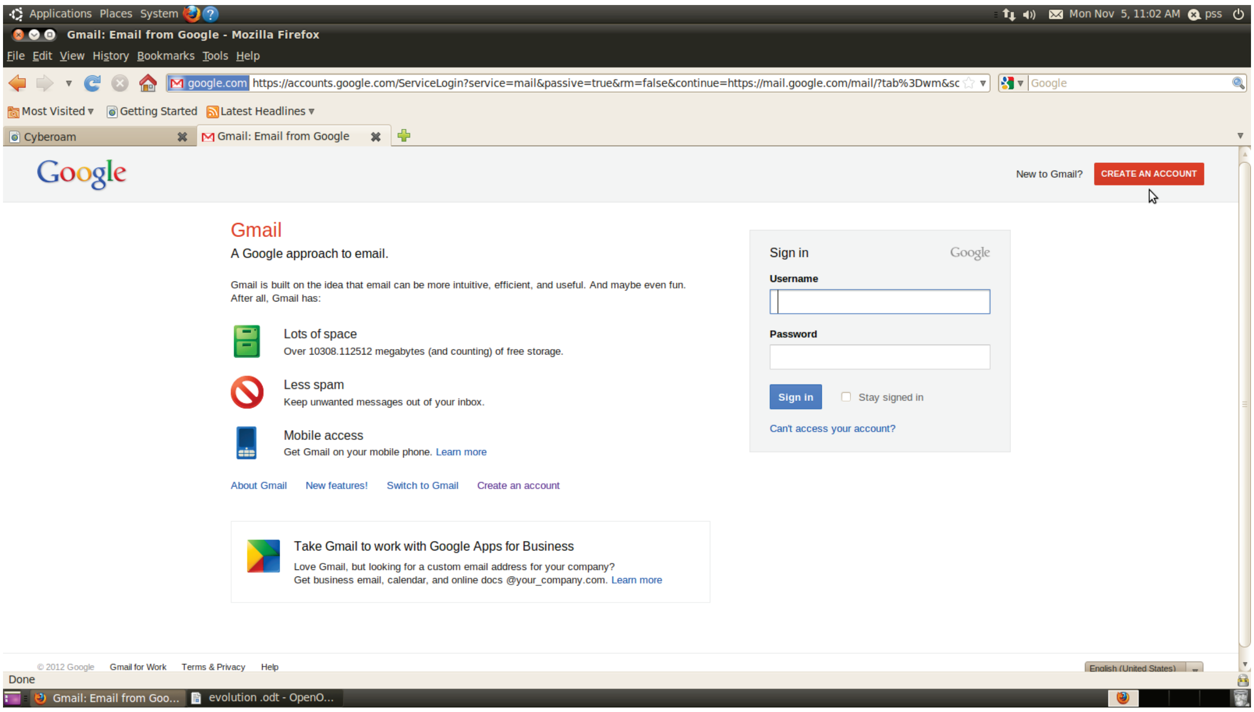
આકૃતિ 14.4 : નવું એકાઉન્ટ બનાવવું

Create New Account લિંક પર ક્લિક આપવાથી નીચેની આકૃતિ 14.5માં દર્શાવેલ દૃશ્ય ઉપલબ્ધ બનશે.



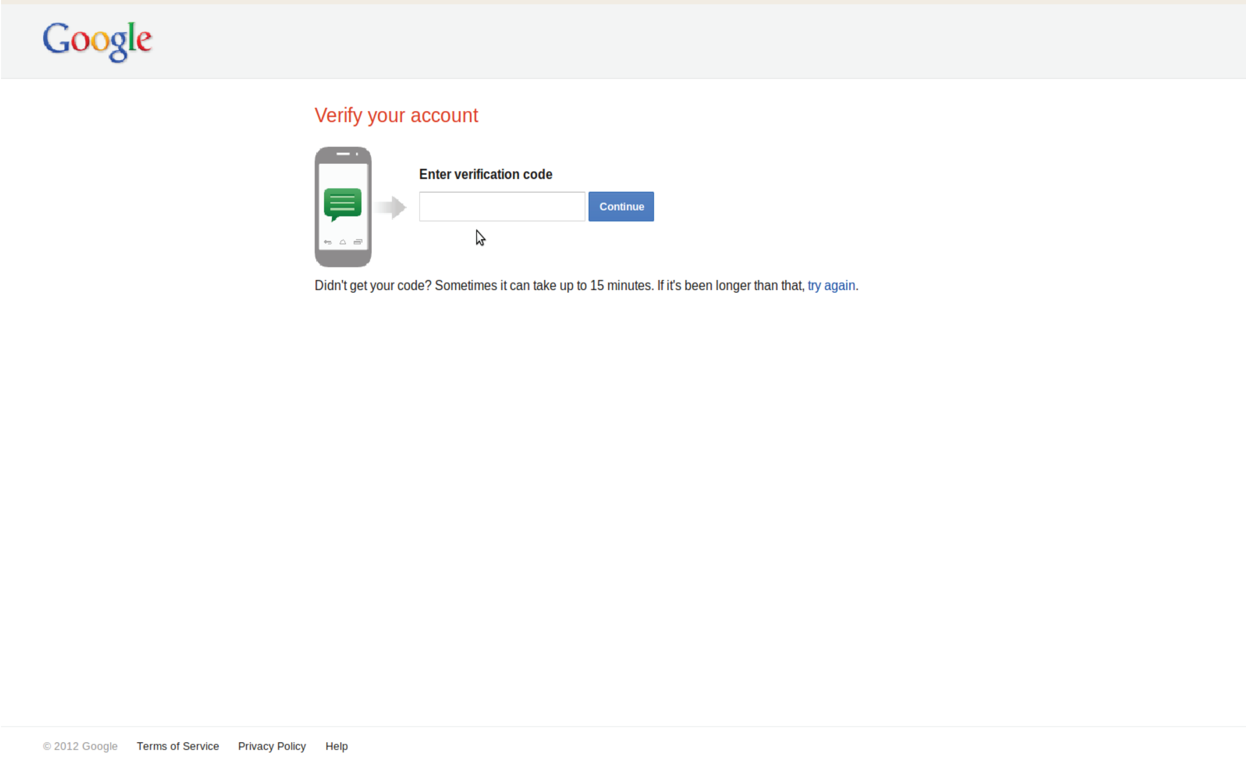
આકૃતિ 14.3 : ઈ-મેઈલ એકાઉન્ટ બનાવવા માટે Gmail પસંદ કરવું

આકૃતિ 14.4માં દર્શાવ્યા પ્રમાણેનું દૃશ્ય જોવા મળશે. અહીં Create New Account પર ક્લિક કરો.



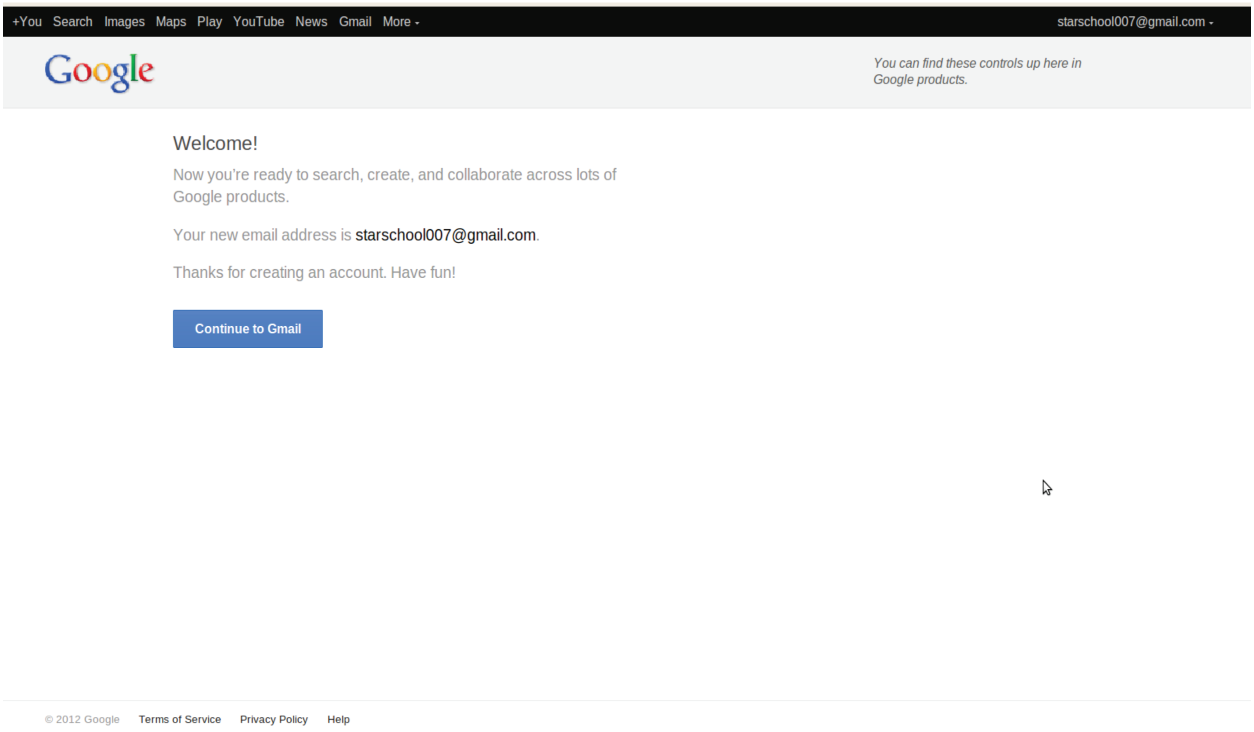
આકૃતિ 14.4 : નવું એકાઉન્ટ બનાવવું

Create New Account લિંક પર ક્લિક કરવાથી નીચેની આકૃતિ 14.5માં દર્શાવેલ દૃશ્ય ઉપલબ્ધ બનશે.



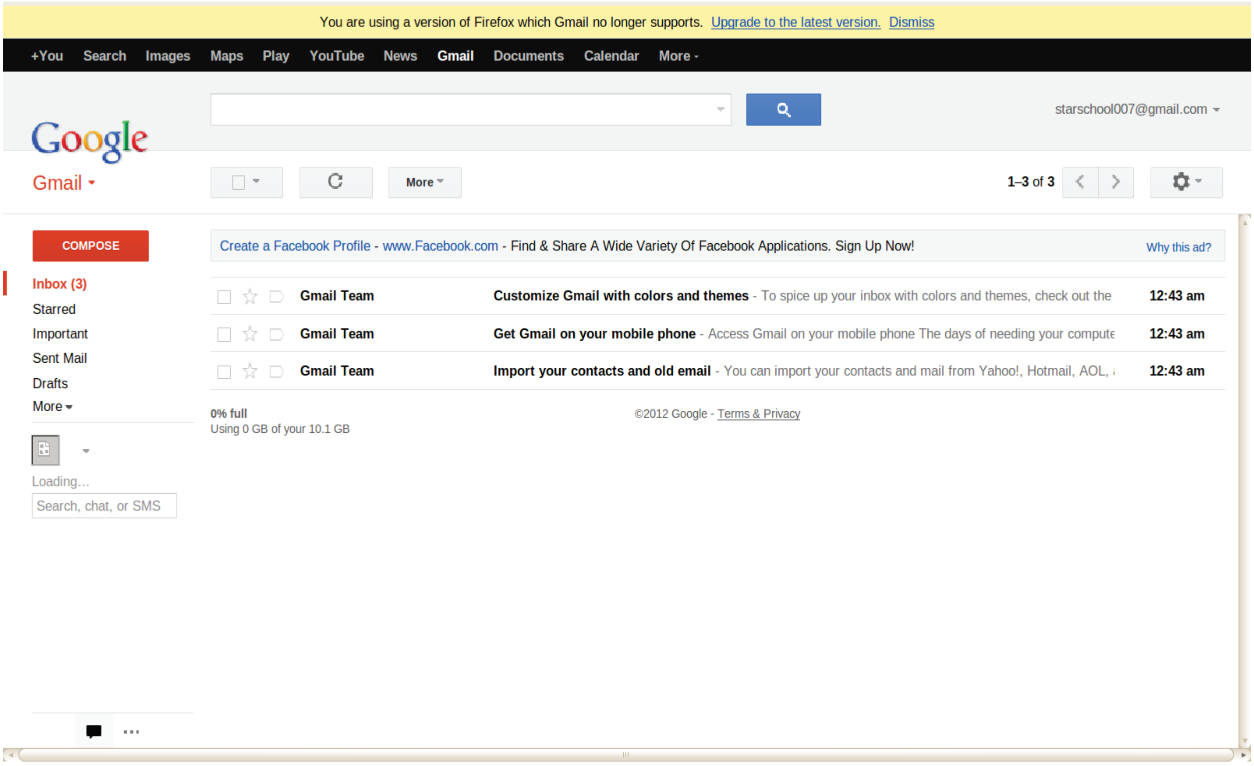
આકૃતિ 14.7 : વેરીફિકેશન કોડ પૂરો પાડવો

અહીં મોકલવામાં આવેલ વેરીફિકેશન કોડ પૂરો પાડવો જરૂરી છે. ત્યાર બાદ આકૃતિ 14.8 માં દર્શાવેલ આવકારસંદેશ જોવા મળશે.



આકૃતિ 14.8 : ગૂગલ તરફથી આવકારસંદેશ

અહીં continue પસંદ કરવાથી આકૃતિ 14.9માં દર્શાવેલ સ્ક્રીન પ્રસ્તુત કરવામાં આવશે.



આકૃતિ 14.9 : Gmail એકાઉન્ટ બની ગયા પછી

ઈ-મેઈલ એકાઉન્ટ બની જાય તે પછી ઈ-મેઈલ આઈડી મિત્રો અને પરિચિતોને આપી શકાય છે. આ જ રીતે, yahoo, rediffmail કે hotmail જેવી જુદી-જુદી ઈ-મેઈલ સેવા પૂરી પાડનાર વેબસાઈટની મદદથી પણ ઈ-મેઈલ એકાઉન્ટ બનાવી શકાય છે.

ઈવૉલ્યુશન - મેઈલ-ક્લાયન્ટ (Evolution as Mail Client) :

'ઈ-મેઈલ ક્લાયન્ટ' એ અંગત કમ્પ્યૂટર પર સક્રિય એક એવો વિનિયોગ છે, જેનો ઈ-મેઈલને મોકલવા, મેળવવા અને સંગ્રહ કરવા માટે ઉપયોગ કરી શકાય. ઈ-મેઈલ માટેના આવા અનેક ક્લાયન્ટ ઉપલબ્ધ છે. ઈ-મેઈલની મૂળભૂત સુવિધા પૂરી પાડવા ઉપરાંત કેટલાંક ઈ-મેઈલ ક્લાયન્ટ અન્ય સુવિધાઓ પણ પૂરી પાડે છે. જેવી કે, ત્વરિત શોધ, એડવાન્સ મેસેજ ફિલ્ટરિંગ, સંદેશાઓનાં જૂથ બનાવવા, શોધેલા સંદેશા કે મદદના પરિણામને લેબલ આપવાં વગેરે. થન્ડરબર્ડ (Thunderbird), ઈવૉલ્યુશન (Evolution), ક્લૉઝ મેઈલ (Claws Mail), કે-મેઈલ (Kmail), બાલસા (Balsa), મટ્ટ (Mutt) અને પાઈન (Pine) ઈ-મેઈલ ક્લાયન્ટનાં ઉદાહરણો છે.

ઈવૉલ્યુશન એ માહિતીની કાર્યક્ષમ રીતે વ્યવસ્થા કરતો એક ઈ-મેઈલ ક્લાયન્ટ છે. જે એક જ સ્થાને ઈ-મેઈલ, ઍડ્રેસબુક, કૅલેન્ડર અને અન્ય કાર્યોના સંચાલનની સુવિધા પૂરી પાડે છે. તે (સ્પામ કે જન્ક જેવા) બિનજરૂરી ઈ-મેઈલને સલામતીપૂર્વક અટકાવી શકે છે. તેને એક ગ્રુપવેર ઍપ્લિકેશન (Groupware Application) તરીકે ગણવામાં આવે છે. (ગ્રુપવેર ઍપ્લિકેશન વ્યક્તિઓના કોઈ જૂથને સાથે મળીને કાર્ય કરવાની સુવિધા પૂરી પાડે છે.)

મેઈલ-ક્લાયન્ટનો ઉપયોગ કરવાથી ઘણા લાભ મળે છે. તેમાંના કેટલાંક નીચે દર્શાવ્યા છે :

- ઈ-મેઈલ ક્લાયન્ટનો ઉપયોગ કરવામાં આવે તો ઈન્ટરનેટ સાથે સતત જોડાયેલા રહેવું જરૂરી નથી. એક વાર જોડાણ કરી, તમામ ઈ-મેઈલ ડાઉનલોડ કરી જોડાણ બંધ કરી દઈ શકાય છે. પછીના અનુકૂળ સમયે આ ઈ-મેઈલ વાંચી શકાય છે. જ્યારે ઈન્ટરનેટ સાથેનું જોડાણ નબળું અથવા અસ્થિર હોય, ત્યારે ખાસ કરીને આ ઘણું ઉપયોગી સિદ્ધ થાય છે.

- કોઈ પણ સમયે ગમે તેટલા ઈ-મેઈલ લખી શકાય છે, તેનો સંગ્રહ કરી શકાય છે અને જ્યારે પણ ઈન્ટરનેટ જોડાણ ઉપલબ્ધ બને ત્યારે તેને મોકલી શકાય છે.
- મેઈલ-ક્લાયન્ટ સામાન્ય રીતે ઘણા ઝડપી હોય છે. તથા ઍડ્રેસબુક, કૅલેન્ડર વગેરે જેવી સુવિધાઓ એક જ સ્થાને પૂરી પાડે છે.
- ઈ-મેઈલને લગતા અનેક વિનિયોગો જ નહીં, પરંતુ એક જ વાર પ્રસ્થાપિત કર્યા પછી અનેક ઈ-મેઈલ એકાઉન્ટને તે એક જ સ્થળેથી સંચાલિત કરવાની સુવિધા આપે છે.

જોકે, એક કે વધુ ઈ-મેઈલ એકાઉન્ટના સંચાલન માટે કમ્પ્યૂટર પર વિશિષ્ટ સૉફ્ટવેરની પ્રસ્થાપના અને સંરચના જરૂરી છે. તદ્ઉપરાંત, આ ક્લાયન્ટ કમ્પ્યૂટરમાં સંદેશાઓનો સંગ્રહ પણ કરે છે, જેને કમ્પ્યૂટરનો કોઈ પણ ઉપયોગકર્તા વાંચી શકે છે.

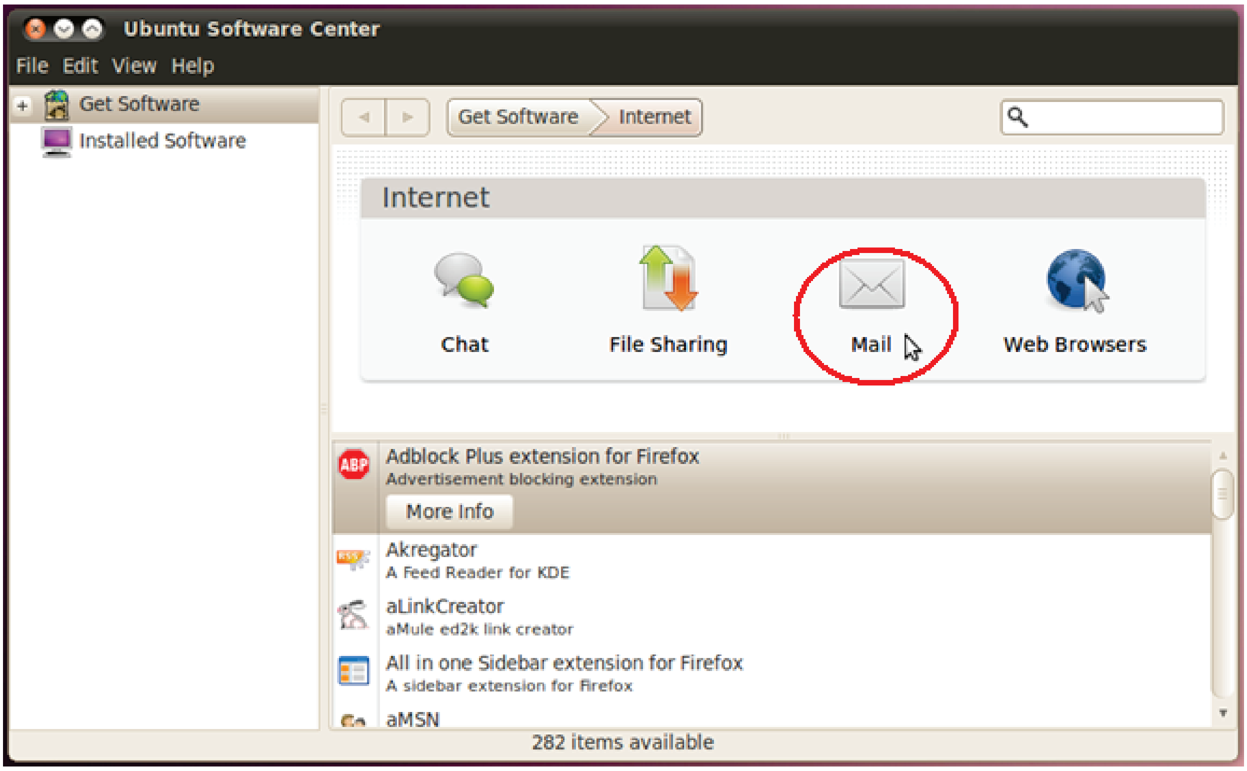
Evolution ક્લાયન્ટને ઉબુન્ટુની મુખ્ય સ્ક્રીન પર આવેલા 'Applications' મેનૂમાંથી સીધું જ પસંદ કરી શકાય છે. જો આ સૉફ્ટવેર ઉપલબ્ધ ન હોય, તો નીચેની જણાવેલ ક્રમને અનુસરી ઉબુન્ટુ સૉફ્ટવેર સેન્ટર દ્વારા તેને પ્રાપ્ત કરી શકાય છે :

ઈવૉલ્યુશન મેળવવું (Getting Evolution) :

- Applications મેનૂ ખોલો.
- ઉબુન્ટુ સૉફ્ટવેર સેન્ટરમાં જઈ આકૃતિ 14.10માં દર્શાવ્યા મુજબ Internet client પસંદ કરો :

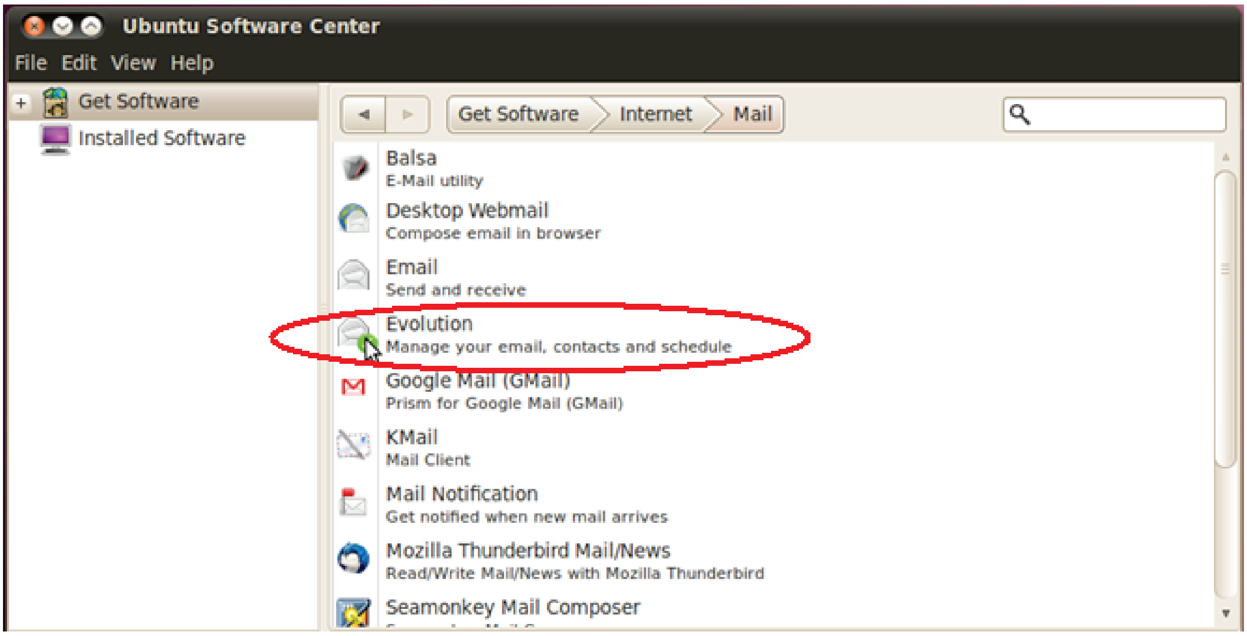
આકૃતિ 14.10 : ઈવૉલ્યુશન જેવું ઈન્ટરનેટ સંબંધિત સૉફ્ટવેર મેળવવું

આકૃતિ 14.10માં દર્શાવેલ 'Internet' આઈકન પર ક્લિક કરવામાં આવે, ત્યારે આકૃતિ 14.11માં દર્શાવેલ સ્ક્રીન જોવા મળે છે.



આકૃતિ 14.11 : મેઇલ-વિકલ્પ પસંદ કરવો

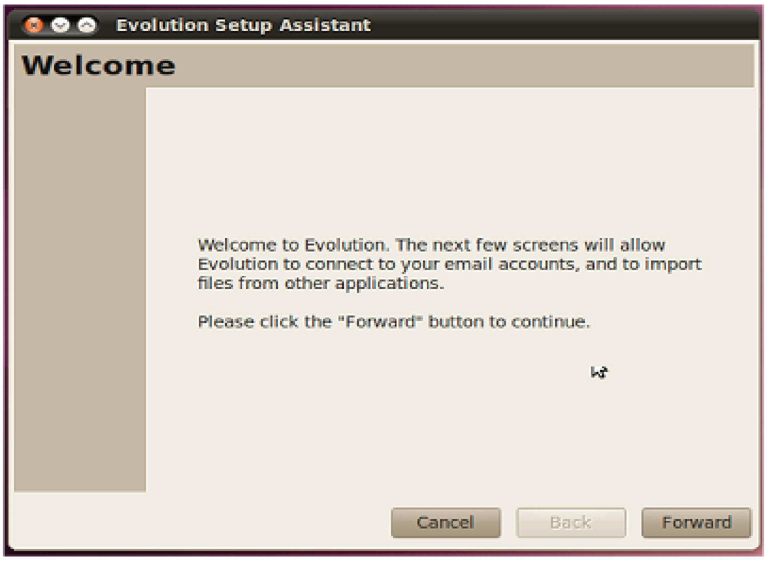
આકૃતિ 14.11માં દર્શાવ્યા મુજબ Mail વિકલ્પ પસંદ કરો. આથી 14.12માં દર્શાવેલ સ્ક્રીન પ્રસ્તુત કરવામાં આવશે.



આકૃતિ 14.12 : મેઇલ-ક્લાયન્ટ તરીકે ઇવૉલ્યુશનની પસંદગી

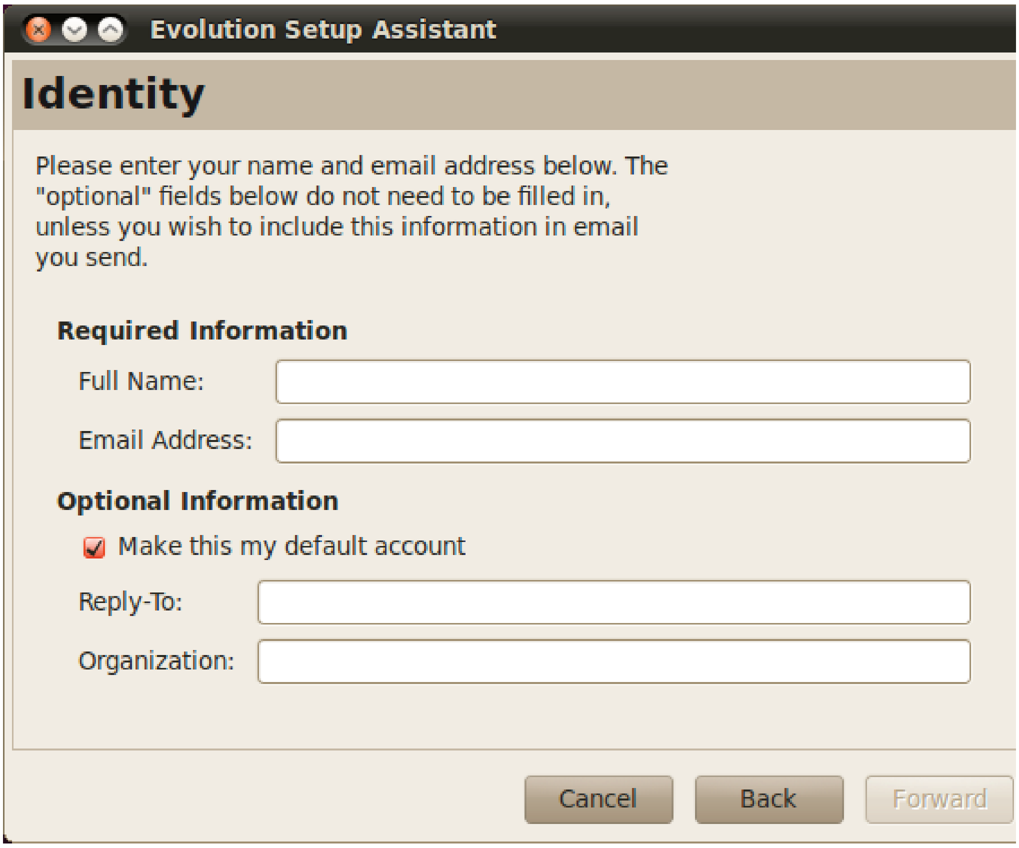
ઇવૉલ્યુશનની સંરચના કરવી (Configuration of Evolution) :

ઇવૉલ્યુશન મેઇલ-ક્લાયન્ટ મેળવ્યા બાદ, નીચે મુજબ તેની સંરચના કરવી જરૂરી બને છે. ઇવૉલ્યુશનની આવકાર સ્ક્રીન ખોલવા માટે Applications → Office → Evolution Mail અને Calendar વિકલ્પ પસંદ કરો. આમ કરવાથી આકૃતિ 14.13માં દર્શાવેલ આવકારસંદેશ જોવા મળશે.



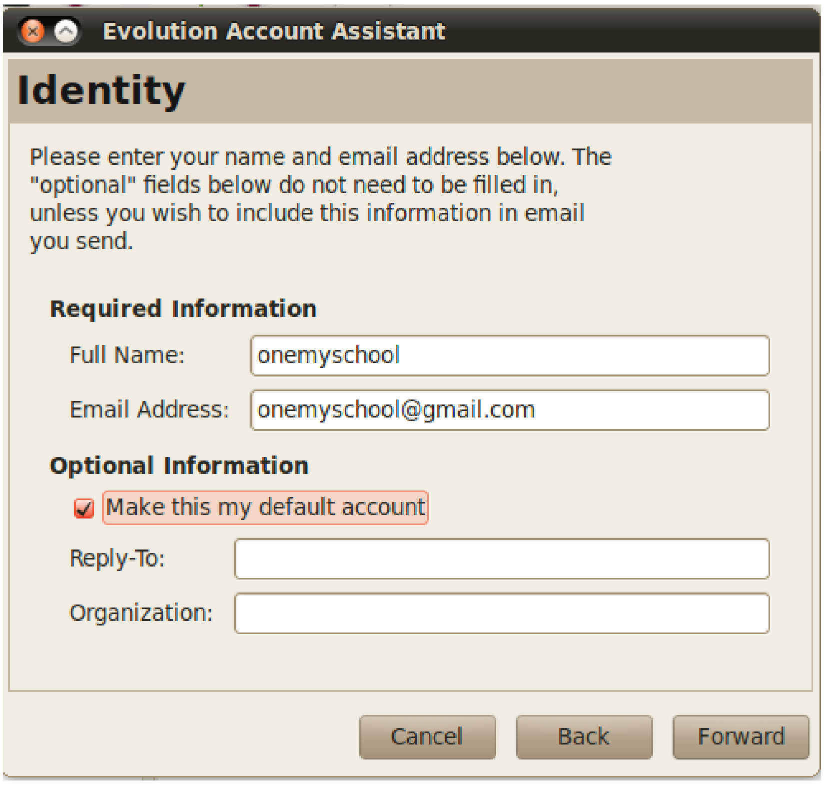
આકૃતિ 14.13 : ઇવૉલ્યુશનની સંરચના સમયે આવકારસંદેશ

હવે, ‘Forward’ બટન પર ક્લિક આપવાથી રજૂ થયેલ સ્ક્રીન દ્વારા બૅકઅપ તરીકે રાખેલી વિગતોને રી-સ્ટોર કરવા માટે પૂછવામાં આવશે. બૅકઅપ લઈ રાખ્યો હોય તેવી સ્થિતિમાં જો કોઈ મુશ્કેલીને કારણે ઇવૉલ્યુશનની પુનઃસંરચના કરતા હોઈએ ત્યારે આ ઘણું મદદરૂપ બને છે. જો પ્રથમ વખતનું પ્રસ્થાપન હોય, તો Forward બટન પર ક્લિક આપવાથી આકૃતિ 14.14માં દર્શાવ્યા મુજબનો સ્ક્રીન પ્રદર્શિત થશે.



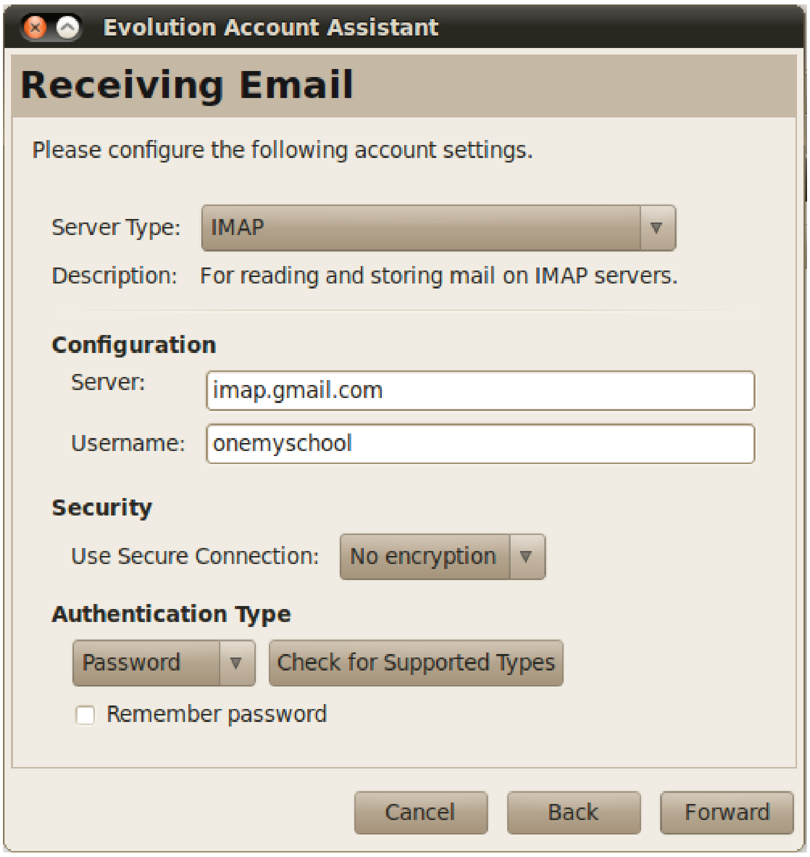
આકૃતિ 14.14 : ઇવૉલ્યુશનની મેઇલ-ક્લાયન્ટ માટે આઇડેન્ટિટી નક્કી કરવી

અહીં સંદેશ મોકલનાર તથા તેની સંસ્થાની ઓળખ (identity) માટે જરૂરી એવી કેટલીક માહિતી પૂરી પાડવામાં આવે છે. આકૃતિ 14.15માં આવી કેટલીક નમૂનારૂપ માહિતી દર્શાવવામાં આવેલી છે.



આકૃતિ 14.15 : ઈવૉલ્યુશન મેઈલ-ક્લાયન્ટ માટે

હવે 'Forward' બટન પર ક્લિક આપવાથી આકૃતિ 14.16માં દર્શાવ્યા મુજબનો સ્ક્રીન જોવા મળશે.

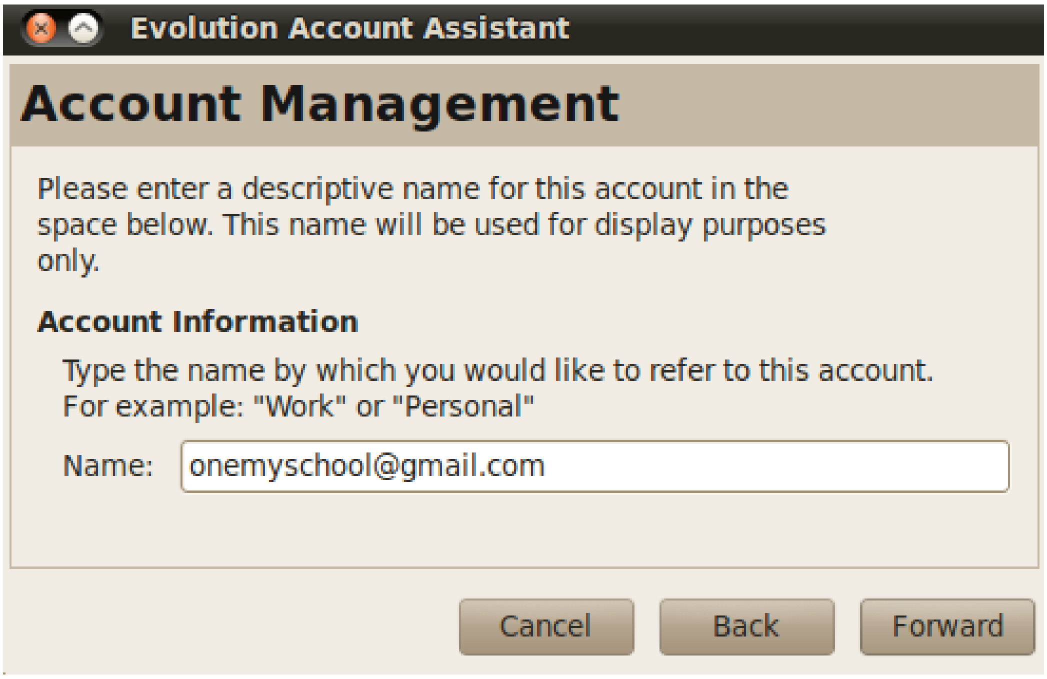


આકૃતિ 14.16 : ઈવૉલ્યુશનને સર્વર અંગેની માહિતી પૂરી પાડવી

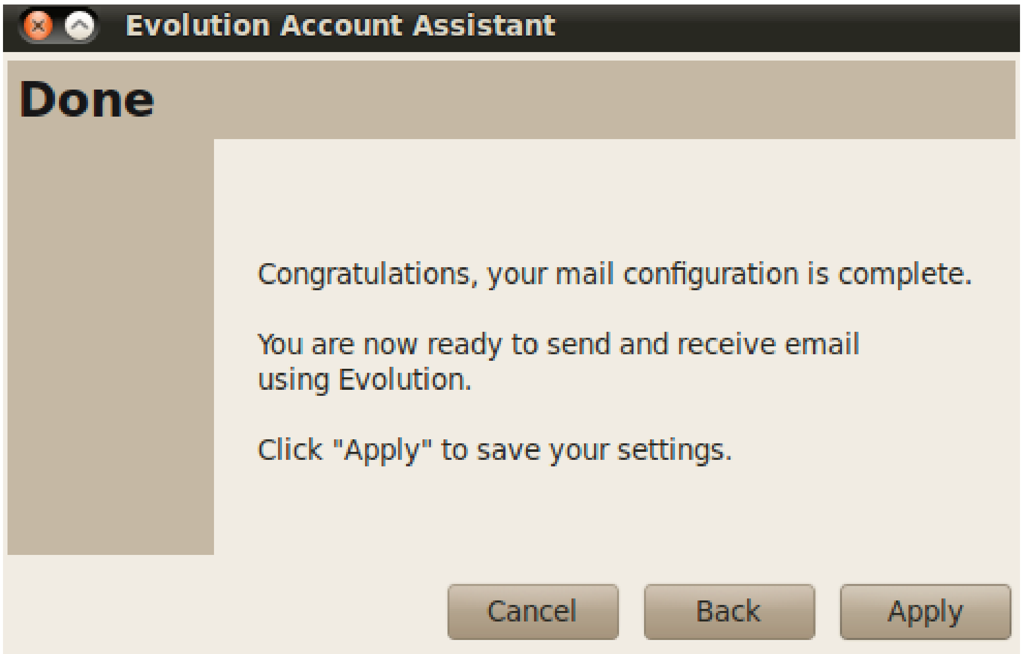
આપણે Gmail એકાઉન્ટની સંરચના કરતા હોવાથી સર્વરના નામ તરીકે imap.gmail.com ઉમેરવું જોઈએ. જુદા-જુદા ઍકાઉન્ટ જો ઇવૉલ્યુશનમાં ઉમેરવા માંગતા હોઈએ, તો ઇન્ટરનેટ સર્વિસ પ્રોવાઇડર પાસેથી સંદેશા મેળવવા તથા મોકલવા એમ બંને માટેના સર્વરનું નામ જાણવું જરૂરી બને છે. માહિતી ઉમેરાઈ ગયા બાદ Forward બટન પર ક્લિક કરો. આમ કરવાથી ઈ-મેઇલ મેળવવા માટેના વિકલ્પો દર્શાવતા સ્ક્રીન રજૂ કરવામાં આવશે. અહીં ઈ-મેઇલ-ક્લાયન્ટને રિફ્રેશ કરવાનો સમય અને એવી કેટલીક માહિતી ઉમેરવામાં આવે છે.

Forward બટન પર ક્લિક કરવાથી ક્રમાનુસાર આકૃતિ 14.17, આકૃતિ 14.18, આકૃતિ 14.19 અને આકૃતિ 14.20 પર દર્શાવેલ સ્ક્રીન રજૂ કરવામાં આવશે. અંતિમ સ્ક્રીન પર 'Done' સંદેશ દર્શાવવામાં આવશે. 'Apply' બટન પર ક્લિક આપવાથી આ તમામ સંરચનાઓ લાગુ પાડી શકાય છે.

આકૃતિ 14.17 : ઇવૉલ્યુશન માટે સર્વર તથા સુરક્ષા અંગેના વિકલ્પો ગોઠવવા

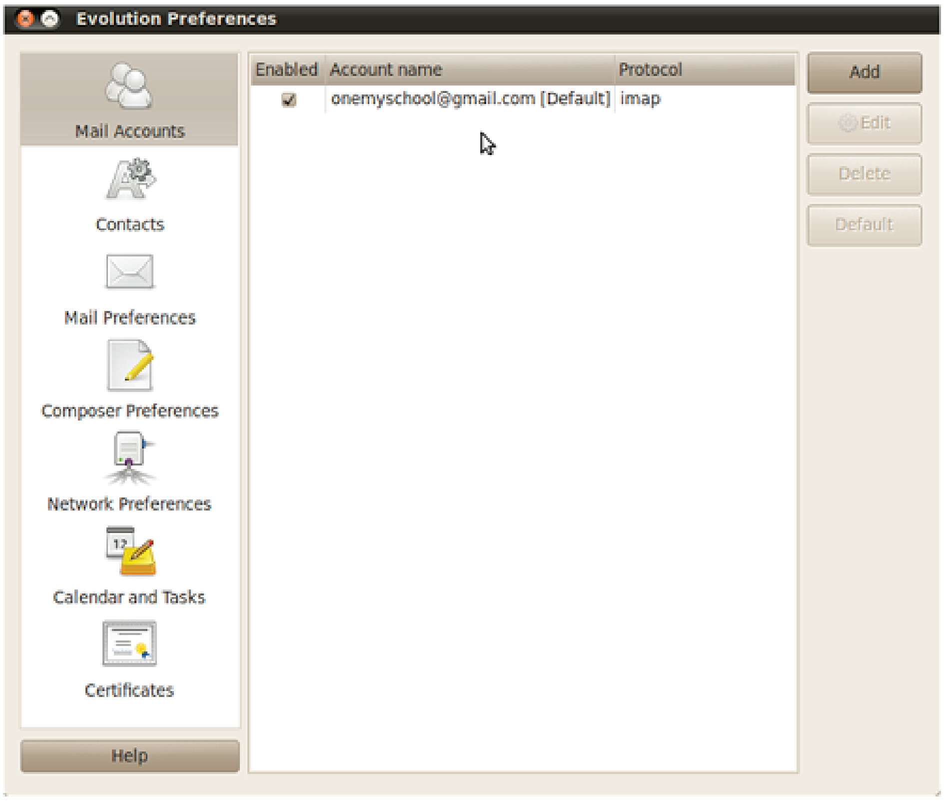


આકૃતિ 14.18 : ઈવૉલ્યુશનમાં એકાઉન્ટની વિગતોનું સંચાલન કરવું



આકૃતિ 14.19 : ઈવૉલ્યુશનમાં સંરચના લાગુ પાડવી

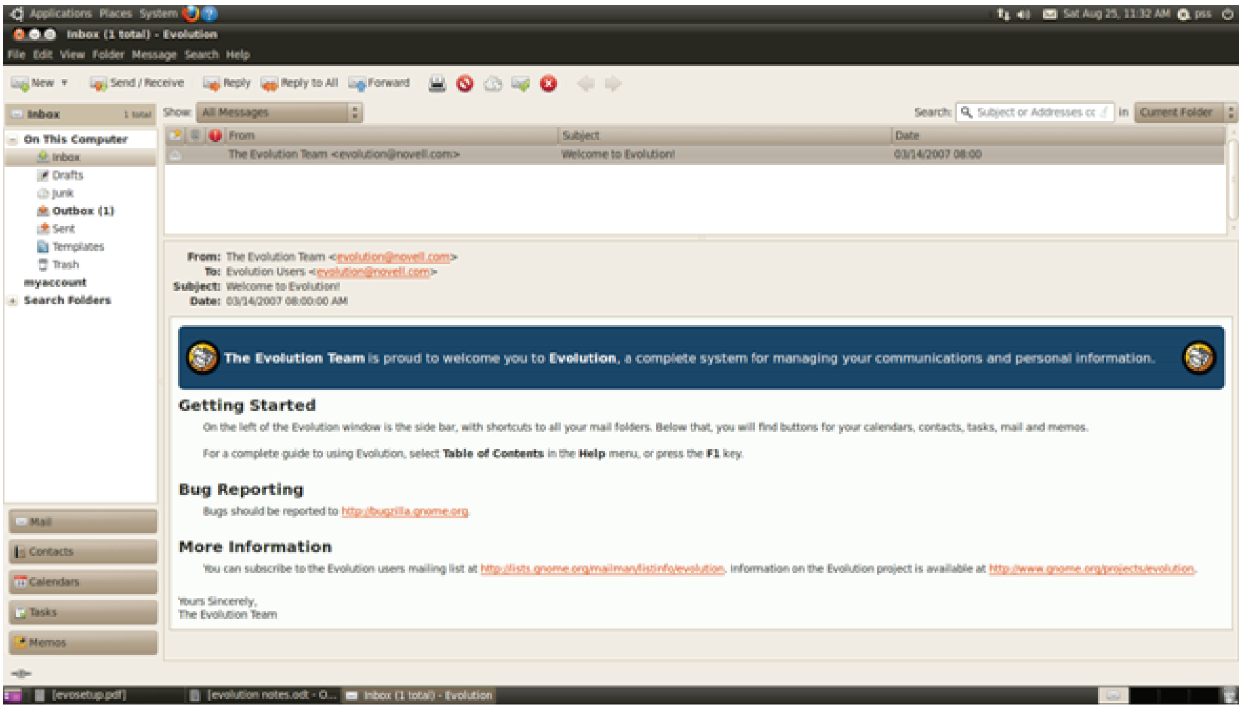
ઉપરનાં પગલાં દ્વારા મેઈલ-એકાઉન્ટની પદ્ધતિસર સંરચના કરી શકાય છે. એક વાર ઈ-મેઈલ ક્લાયન્ટ યોગ્ય રીતે ગોઠવાઈ ગયા પછી સ્વાગતસંદેશ દર્શાવવામાં આવે છે. આ દરમિયાન જો કોઈ માહિતી પૂરી પાડવાનું રહી ગયું હોય, તો 'Edit' મેનૂના 'Preferences' વિકલ્પનો ઉપયોગ કરી શકાય છે. આકૃતિ 14.20માં દર્શાવેલ સ્ક્રીન જુઓ.



આકૃતિ 14.20 : ઈવૉલ્યુશનની પસંદગી બદલવી

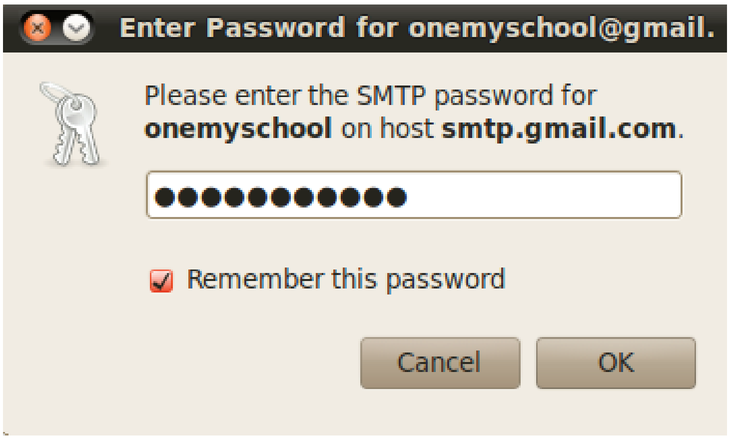
આ વિકલ્પ દ્વારા મેઈલ, સંપર્ક, નેટવર્ક, કૅલેન્ડર અને અન્ય કાર્યો માટે પસંદગીની સંરચના કરી શકાય છે.

અહીં આપણે સંરચનાના હેતુ માટે એક કામચલાઉ એકાઉન્ટનો ઉપયોગ કર્યો છે. જો તમારી પાસે યોગ્ય ઈ-મેઈલ સરનામું હોય, તો તમે મેઈલ-ક્લાયન્ટનો ઉપયોગ શરૂ કરી શકો છો. ઈ-મેઈલ ક્લાયન્ટનો દેખાવ લગભગ આકૃતિ 14.21માં દર્શાવેલ દેખાવને મળતો આવે છે.



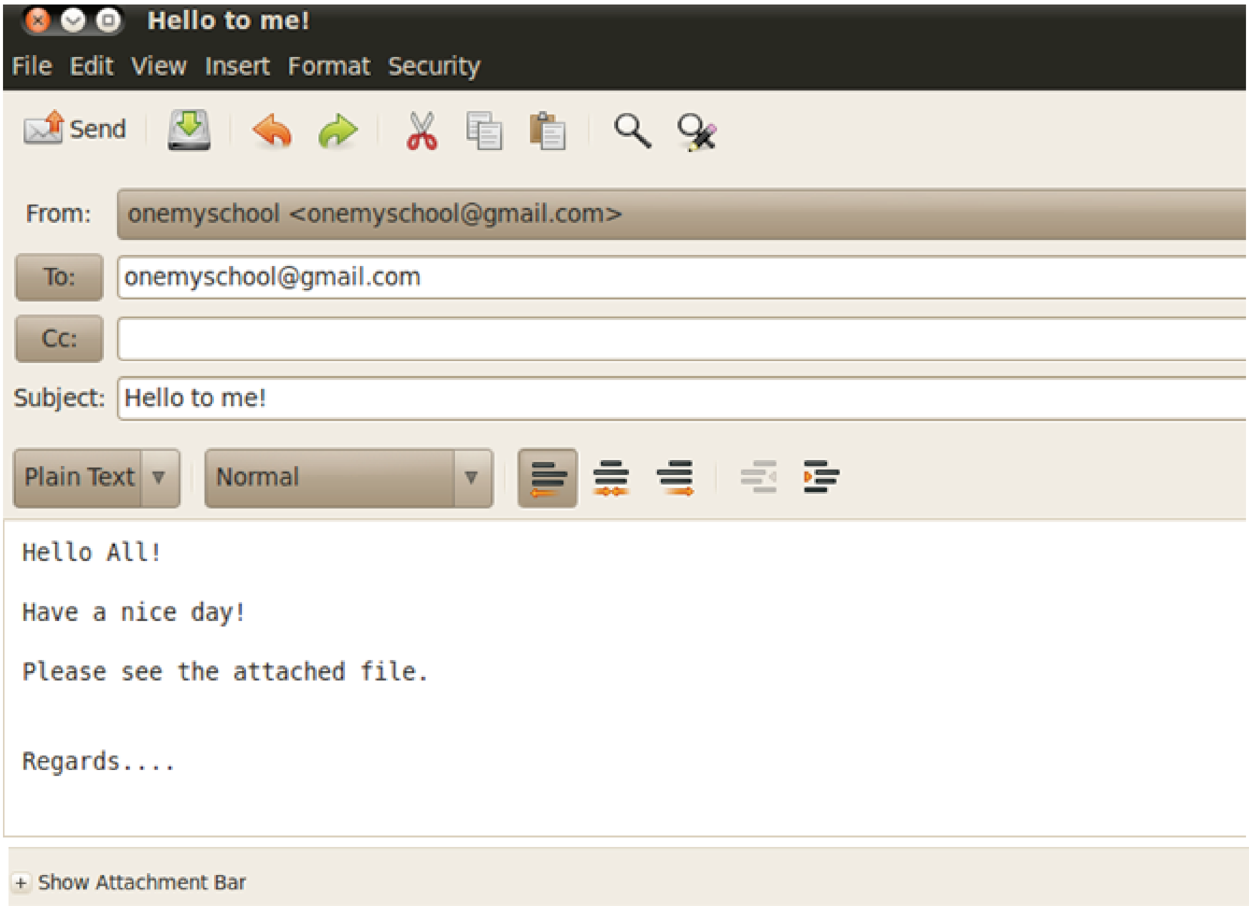
આકૃતિ 14.21 : ઈવૉલ્યુશન ટીમ તરફથી મળેલ પ્રથમ સ્વાગતસંદેશ

અહીં અગાઉનો પાસવર્ડ માંગવામાં આવી શકે છે. આકૃતિ 14.22માં દર્શાવેલ ડાયલૉગબૉક્સ જુઓ. સિસ્ટમ પાસવર્ડને યાદ પણ રાખી શકે છે. પરંતુ જો જાહેર કમ્પ્યૂટર પર કાર્ય કરતા હોઈએ તો પાસવર્ડને યાદ રાખનાર વિકલ્પને રદ કરવો હિતાવહ છે.



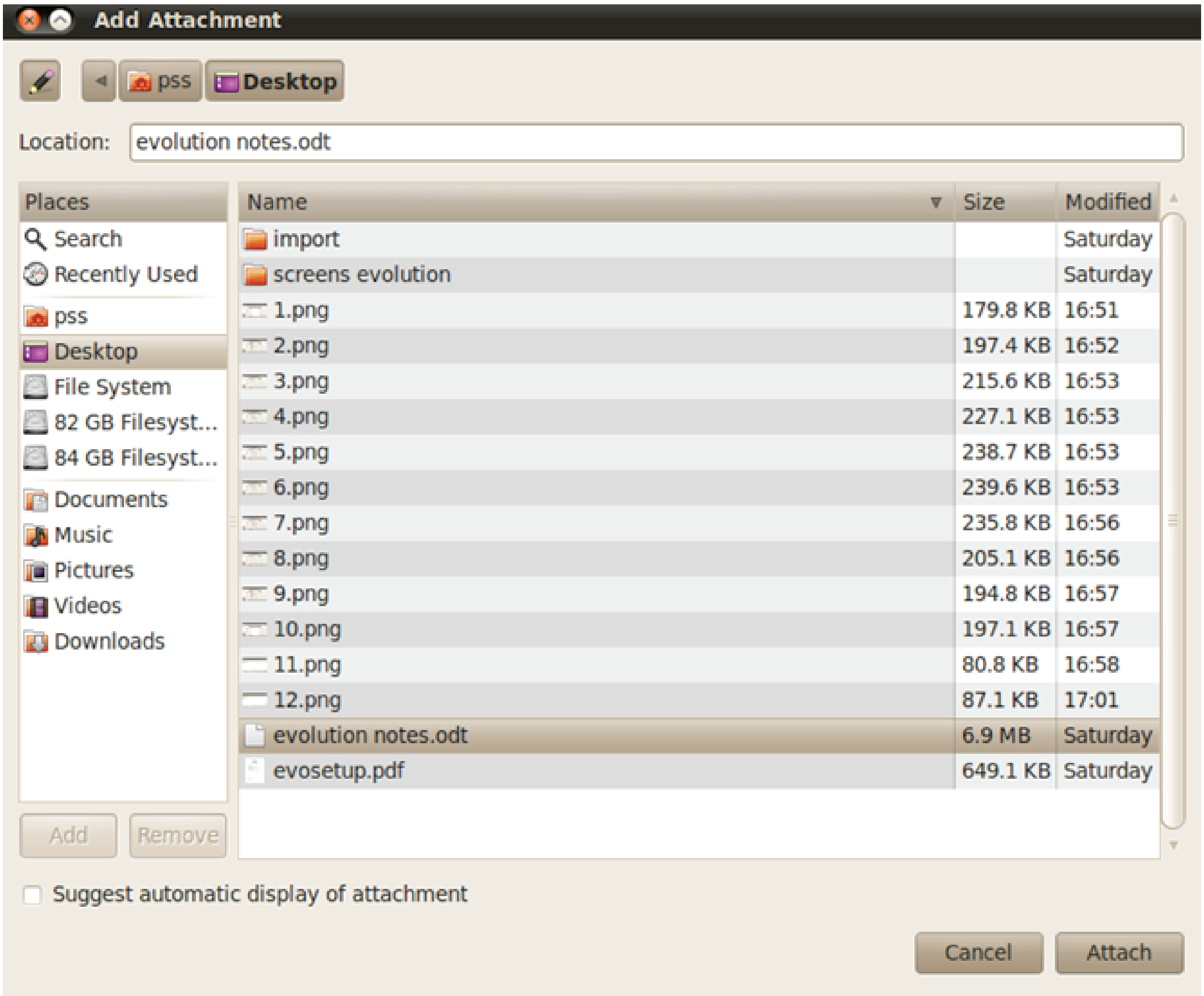
આકૃતિ 14.22 : પાસવર્ડ ઉમેરવો

આકૃતિ 14.23માં નવો ઈ-મેઈલ લખવા માટેનો વિકલ્પ દર્શાવ્યો છે.



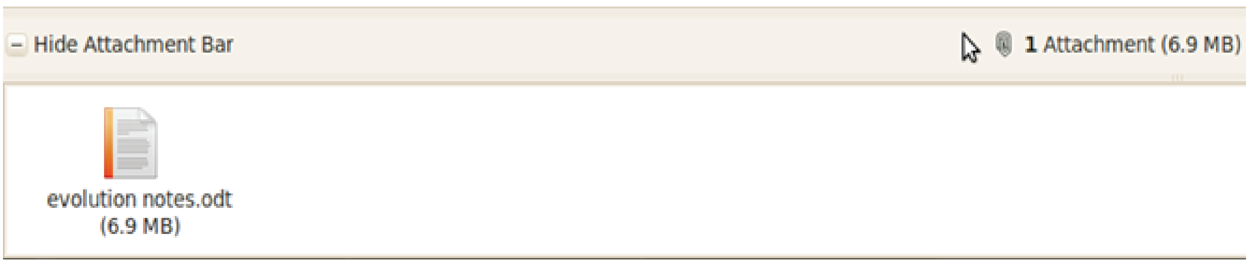
આકૃતિ 14.23 : ઈ-મેઈલ લખવો

ઈ-મેઈલ સાથે ફાઈલનું બિડાણ કરવા માટે Show Attachment બાર પર ક્લિક કરો. આથી 'Attachment' બટન જોવા મળશે. તેની પર ક્લિક કરવાથી બિડાણ કરવાની હોય તે ફાઈલનું નામ અને સ્થાન માંગવામાં આવશે. આકૃતિ 14.24 જુઓ. એ નોંધવું જરૂરી છે કે તમે પસંદ કરેલ ફાઈલ અનુસાર સ્કીનનો દેખાવ જુદો હોઈ શકે છે.



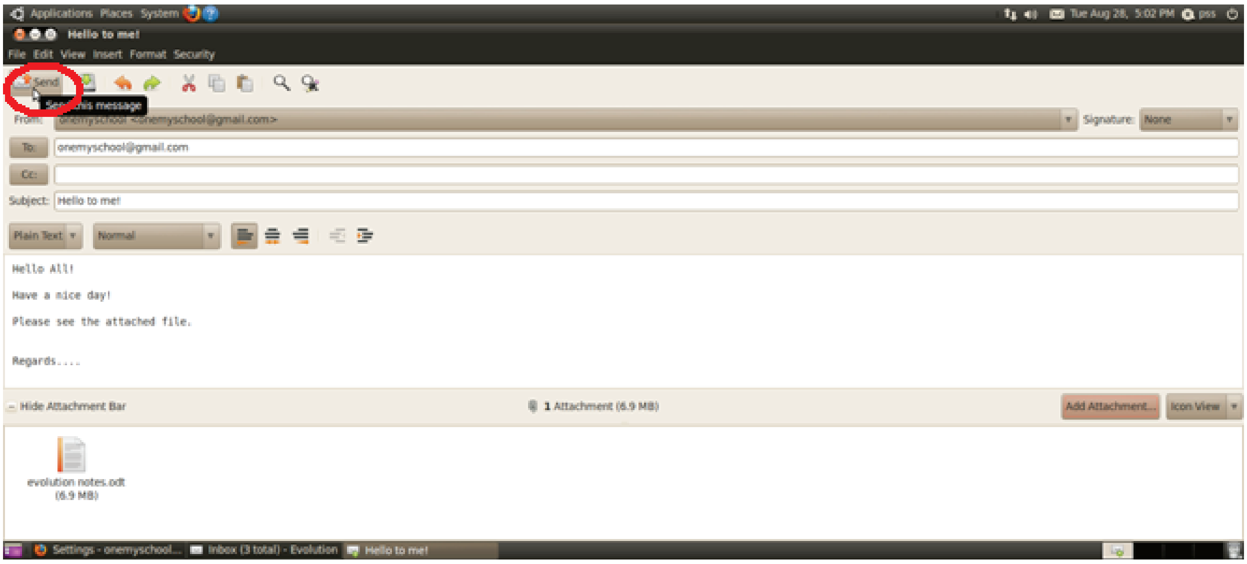
આકૃતિ 14.24 : ઈ-મેઈલ સાથે ફાઈલનું જોડાણ કરવું

એક વાર યોગ્ય ફાઈલ (અહીં 6.9 mb કદ ધરાવતી evolution notes.odt ફાઈલ) પસંદ કરવાથી આકૃતિ 14.25માં દર્શાવ્યા મુજબ તેને સંદેશ સાથે જોડી શકાય છે.



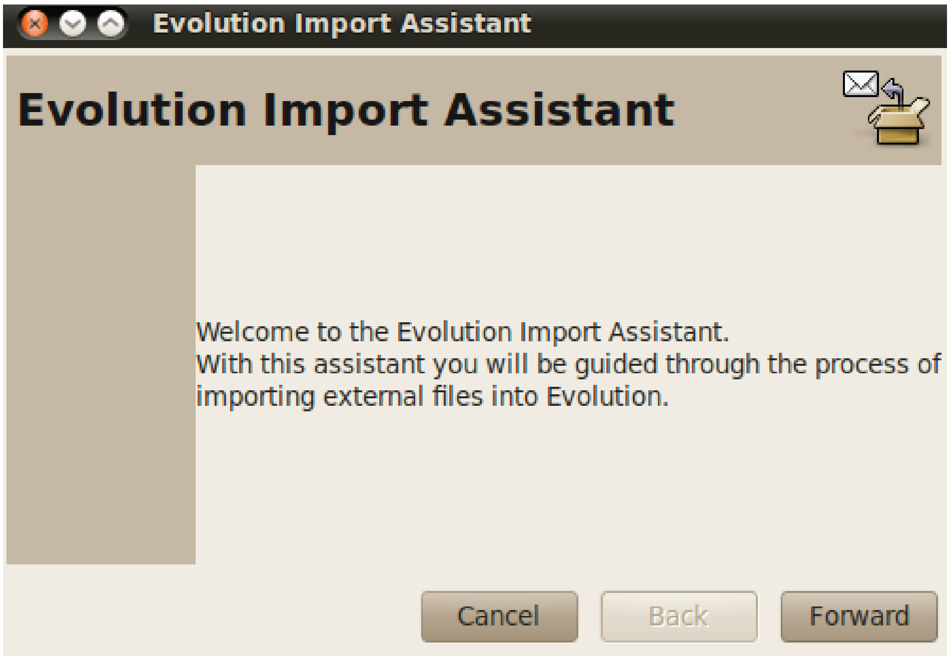
આકૃતિ 14.25 : ઍટેચમેન્ટ બાર

તૈયાર કરેલ સંદેશને મોકલવા માટે આકૃતિ 14.26 માં દર્શાવ્યા મુજબ send બટન પર ક્લિક કરવામાં આવે છે.



આકૃતિ 14.26 : સંદેશ મોકલવો

અન્ય ક્લાયન્ટ પાસેથી સંગૃહીત સંદેશા અને સંપર્ક આયાત કરવા માટે પણ ઈવૉલ્યુશન મદદરૂપ બને છે. હયાત મેઈલ એકાઉન્ટમાંથી સંપર્ક આયાત કરવા માટે આકૃતિ 14.27માં દર્શાવેલ *Evolution Import Assistant* નો ઉપયોગ કરી માહિતી પૂરી પાડો.



આકૃતિ 14.27 : માહિતી આયાત કરવી

Evolution Import Assistant નો ઉપયોગ કરી ક્રમબદ્ધ પગલાંનું માર્ગદર્શન મેળવી શકાય. આ ક્રમને પૂર્ણ કરવાથી જુદી-જુદી ફાઈલોમાં રહેલ સંપર્ક આયાત થઈ શકશે.

સુરક્ષા અને સાંકેતિકરણ (Security and Cryptography) :

જાહેર ડોમેઈન દ્વારા માહિતી તથા સ્રોતની વહેંચણી વખતે માત્ર અધિકૃત વ્યક્તિ જ તેનો ઉપયોગ કરી શકે એવો વિશ્વાસ હોવો જરૂરી છે. ધારો કે આપણે ઈન્ટરનેટ પર વેબસાઈટનો ઉપયોગ કરી ઑનલાઈન બૅન્કિંગ સિસ્ટમ વિકસાવી હોય,

તો માત્ર અધિકૃત ઉપયોગકર્તા જ બૅન્કના તે ખાતાનો ઉપયોગ કરે તેની ખાતરી ઇચ્છનીય છે. અન્યથા, કોઈક અનધીકૃત વ્યક્તિ દ્વારા છેતરપિંડી થઈ શકે અને બૅન્કની સેવા વધુ સમય વિશ્વસનીય રહી શકે નહીં. આ બાબત કોઈ પણ વ્યવસાય માટે વિનાશક સિદ્ધ થઈ શકે છે. વિદ્યાર્થીઓના ગુણાંક, આર્થિક માહિતી, સંરક્ષણ અને અન્ય લશ્કરી ગતિવિધિઓ, ખાદ્ય-પદાર્થો અને દવાઓ બનાવવાની પદ્ધતિ કે માહિતીને માત્ર પસંદગીનાં ક્ષેત્રો પૂરતી જ વિતરીત કરવાની હોય છે. ઇન્ટરનેટ દ્વારા આખી દુનિયામાં ભૌગોલિક મર્યાદા વગર માહિતી અને સેવા વહેંચી શકાય છે, પરંતુ તેની સાથે કોઈ છેતરપીંડી કે ષડ્યંત્રની શક્યતા પણ રહેલી છે. ક્યારેક કોઈ અજ્ઞાત વ્યક્તિ દ્વારા કોઈ સાઇટ હૅક કરવામાં આવી એમ તમે સાંભળ્યું હશે. આવા હૅકર્સથી આપણી મૂલ્યવાન વિગતો સુરક્ષિત રહેવી જોઈએ. ઇન્ટરનેટનો ઉપયોગ કરી સ્રોત અને સેવાની વહેંચણીનો લાભ લેવાની સાથે હૅકર જેવા અનિચ્છનીય ઉપયોગકર્તાથી થતી વિગતોની હાનિ માટે સલામતીનું ધ્યાન રાખવું પણ જરૂરી છે. સ્રોતના સુરક્ષિત વિતરણ માટે નીચે જણાવેલ માર્ગ મદદરૂપ બને છે :

સંપત્તિ બચાવવી (To Protect Assets) : સંસ્થાના સ્રોત જાહેર ડોમેઇન પર મૂકવામાં આવે, તો તે અનધિકૃત ઉપયોગકર્તાઓથી સુરક્ષિત રહેવા જોઈએ. આ સ્રોતોમાં હાર્ડવેર અને સૉફ્ટવેર ઉપરાંત માહિતીનો પણ સમાવેશ થાય છે. સંરક્ષણ કાર્યાલયની ઑનલાઇન ડૉક્યુમેન્ટ મૅનેજમેન્ટ સિસ્ટમ વિશે વિચારીએ તો જણાશે કે તેમાં રહેલ સંવેદનશીલ દસ્તાવેજો માત્ર નિયત અધિકારીઓ વચ્ચે જ વિતરીત થવા જોઈએ અને એમાં રહેલ માહિતી સામાન્ય જનતા માટે અપ્રાપ્ય હોવી જોઈએ.

સ્પર્ધાત્મક વાતાવરણમાં અચળ રહેવું (To Survive in Competitive Scenario) : સંસ્થામાં યોગ્ય સલામતીનાં પાસાંનો વિકાસ કરવાથી તેના માર્કાની શાખ અને સેવાની ગુણવત્તામાં વધારો થાય છે. ઉચ્ચ ગુણવત્તાની સેવા ઉપયોગકર્તાના સ્વીકાર્યભાવને વધારે છે અને સરખા ઉદ્યોગમાં રહેલી અન્ય સંસ્થાઓ સામે સ્પર્ધાત્મક લાભ મેળવે છે. આર્થિક અને વ્યાવસાયિક (ઇ-કૉમર્સ) વિનિયોગો માટે નેટવર્ક સુરક્ષા ઘણું અગત્યનું પાસું બની રહે છે. ઑનલાઇન ખરીદી માટેની સાઇટ, ટેલિફોન બિલની ચુકવણી અને બૅન્કિંગ સિસ્ટમ એવાં ઉદાહરણ છે, જેમાં માહિતીની યોગ્ય સુરક્ષા વગર ટકી રહેવું મુશ્કેલ બને છે.

ઉપયોગકર્તાને વધુ સારી સેવાઓ પૂરી પાડવી (To Provide Better Services to Users) : સંસ્થાઓએ તેમના ઉપયોગકર્તાઓને સુરક્ષિત સેવાની ખાતરી આપવી જોઈએ. આવા વ્યવહારોની ખાતરી હંમેશા ઇચ્છનીય છે. ઘણી સૉફ્ટવેર બનાવનાર સંસ્થાઓ સુરક્ષાનાં પાસાંને મોટા પ્રમાણમાં અગ્રિમતા આપે છે. આ પ્રકારની ગુણવત્તાનાં ધોરણોમાં વધારો ઉપયોગકર્તાની સંસ્થા પ્રત્યેની વિશ્વસનીયતામાં વધારો કરે છે અને સંસ્થા સાથેના ગ્રાહકના સંબંધોમાં સુધારો લાવે છે. લોકોને સલામત અને વિશ્વસનીય ક્રિયાઓ વધુ માફક આવે છે. જો તમને ખબર પડે કે તમે જે બૅન્ક સાથે વ્યાવસાયિક વ્યવહારો કરી રહ્યા છો, એની વેબસાઇટ ગયા સપ્તાહે હૅક કરી લેવામાં આવી હતી, તો હવે તમે તે બૅન્ક સાથે વધુ વ્યવહાર ચાલુ રાખવાનું પસંદ કરશો ?

સંસ્થામાં સ્રોત અને સેવાઓનું સુવ્યવસ્થિત રીતે સંચાલન કરવામાં આવે તો વિગતોના અધિકૃત ઉપયોગની ખાતરી મેળવી શકાય છે. આ ઉપરાંત પ્રયુક્ત સિસ્ટમની નિર્બળતાઓ જાણવી પણ જરૂરી છે. પ્રયુક્ત સિસ્ટમની નિર્બળતાઓને ભેદ્યતા (vulnerabilities) તરીકે ઓળખવામાં આવે છે. પૂરતા સ્તરોમાં સલામતી તથા સુરક્ષિત વાતાવરણ પૂરું પાડવા માટે કમ્પ્યૂટર સિસ્ટમ (હાર્ડવેર અને સૉફ્ટવેર બંને) અથવા તો ઉપયોગકર્તાને હાનિકર્તા હોય તેવા જુદા-જુદા પ્રકારનાં જોખમો, શક્ય હુમલાઓ અને ધમકીઓ (threats) વિશે જાણકારી હોવી જરૂરી છે.

હુમલાઓ અને ધમકીઓ પૂર્વયોજિત, આકસ્મિક કે પ્રાકૃતિક એવા કોઈ પણ સ્વરૂપના હોઈ શકે છે અને તે સિસ્ટમની કાર્યપદ્ધતિને, નિયોજીકરણને કે અખંડિતતાને હાનિ પહોંચાડી શકે છે. તેનું આક્રમણ સિસ્ટમની નિર્બળતાનો લાભ લેવા માટેની વિશિષ્ટ તક્નિક બની રહે છે.

સિસ્ટમને થઈ શકે તેવા હુમલા અને નુકસાન વિશે સંક્ષિપ્ત ચર્ચા નીચે કરવામાં આવી છે :

વાઈરસ (Virus) :

વાઈરસ એ કોઈ સૉફ્ટવેર સાથે આવતો પરોપજીવી પ્રોગ્રામ છે. ઇન્ટરનેટના કોઈ આકર્ષક સૉફ્ટવેરનો ઉપયોગ કરવામાં આવે છે, ત્યારે તેની સાથે વાઈરસ આવવાની સંભાવના રહેલી છે. જૈવિક વાઈરસની જેમ આ વાઈરસને પણ છુપાઈ રહેવા કે કાર્ય કરવા યજમાનની જરૂર પડે છે. આવા યજમાન-પ્રોગ્રામનો અમલ કરવામાં આવે છે, ત્યારે વાઈરસ ફેલાય છે. જ્યારે મેઇલ કે પેનડ્રાઇવ દ્વારા વાઈરસગ્રસ્ત પ્રોગ્રામનું વિતરણ કરવામાં આવે છે, ત્યારે પ્રોગ્રામ સ્વીકારનાર કમ્પ્યૂટરમાં પણ વાઈરસનો પ્રવેશ થવાની શક્યતા રહેલી છે. કમ્પ્યૂટરમાં પ્રવેશ થયા બાદ તે વાઈરસના ગુણોત્તરની માત્રામાં વૃદ્ધિ થતી રહે છે.

બજારમાં ઉપલબ્ધ એવા વાઈરસ-સ્કેનિંગ પ્રોગ્રામ દ્વારા આ પ્રકારના આક્રમણથી બચી શકાય છે. Clam ઍન્ટિવાઈરસ સૉફ્ટવેર (www.clamwin.com) એ નિ:શુલ્ક સેવા આવતું ઑપનસૉર્સ ઍન્ટિવાઈરસ સૉફ્ટવેર છે. મોટા ભાગના વાઈરસ સ્કેનિંગ પ્રોગ્રામ જાણીતા વાઈરસ સામે અસરકારક હોય છે, પરંતુ દુર્ભાગ્યે તે નવા વાઈરસને ઓળખી કે દૂર કરી શકતા નથી.

ટ્રોજનહૉર્સ (Trojan Horse) :

ટ્રોજનહૉર્સ એક એવા પ્રોગ્રામ અથવા કોડનો ભાગ છે જે કોઈ અન્ય પ્રોગ્રામની અંદર છુપાયેલો રહે છે અને કમ્પ્યૂટરના સ્રોતને હાનિકારક કામગીરી બજાવે છે. 'ટ્રોજનહૉર્સ' નામ પ્રાચીન ગ્રીકની પ્રચલિત ટ્રૉયની કથા પરથી આપવામાં આવ્યું છે. આ કથા મુજબ કિલ્લાના પ્રવેશદ્વારમાં દાખલ થવા માટે લાકડાના એક મોટા ઘોડામાં સૈનિકોને સંતાડી આક્રમણ કરવામાં આવે છે અને ટ્રૉયને પરાજિત કરવામાં આવે છે. સામાન્ય રીતે હાનિકારક કોડ ધરાવતા ટ્રોજન-પ્રોગ્રામ કેટલીક ઉપયોગી અને આકર્ષક માહિતી સાથે ઉપલબ્ધ બનતા હોય છે. જેમકે, બિડાણ ધરાવતા મેઇલ, સ્ક્રીનસેવર કે નિ:શુલ્ક રમતો. જ્યારે ઉપયોગકર્તા પ્રોગ્રામનો અમલ કરે છે, ત્યારે તેમાં સંતાયેલો પ્રોગ્રામ પણ આપોઆપ સક્રિય બને છે અને તે મુખ્ય પ્રોગ્રામને સમાંતર પોતાનું હાનિકારક કાર્ય કરે છે.

ટ્રોજનહૉર્સનું પ્રચલિત ઉદાહરણ Password Grabber છે. તેમાં login.exe ફાઈલને અન્ય login.exe ફાઈલ સાથે બદલવામાં આવે છે. જે વાસ્તવમાં એક ટ્રોજનહૉર્સ છે. જ્યારે ઉપયોગકર્તા યૂઝરનેમ અને પાસવર્ડ લખે છે, ત્યારે સિસ્ટમ તે માહિતીનો સંગ્રહ કરે છે અને પાસવર્ડ ખોટો હોવાનો સંદેશ પ્રસ્તુત કરે છે. આ દરમિયાન સિસ્ટમ મૂળભૂત login.exeને નિયંત્રણ આપે છે, જે ઉપયોગકર્તા પાસે ફરી યૂઝરનેમ અને પાસવર્ડ માંગે છે. અગાઉ પાસવર્ડ ટાઇપ કરવામાં ભૂલ થઈ હશે તેમ માની ઉપયોગકર્તા નિર્દોષભાવે ફરી પાસવર્ડ પૂરો પાડે છે. અહીં ઉપયોગકર્તાને ખબર હોતી નથી કે તેના યૂઝરનેમ અને પાસવર્ડની ઉઠાંતરી થઈ ચુકી છે.

વૉર્મ (Worm) :

વૉર્મ નુકસાનકારક સૉફ્ટવેર ધરાવતો એક સ્વતંત્ર પ્રોગ્રામ છે. જે સામાન્યત: રોગગ્રસ્ત કમ્પ્યૂટર સાથે જોડાયેલાં નેટવર્કનાં તમામ કમ્પ્યૂટરોમાં પોતાનો ફેલાવો કરે છે. તે નેટવર્ક દ્વારા કમ્પ્યૂટરોનો સંપર્ક કરી તેને નુકસાન પહોંચાડવાની આવડત ધરાવે છે. સ્વયંનો સ્વતંત્રપણે ફેલાવો કરવો એ વાઈરસ અને વૉર્મ વચ્ચેનો મુખ્ય તફાવત છે. વાઈરસ એક સ્વતંત્ર પ્રોગ્રામ નથી; જ્યારે વૉર્મ એક સ્વતંત્ર ફાઈલ છે. જોકે, Mellissa જેવા વાઈરસને વાઈરસ અને વૉર્મની સંયુક્ત લાક્ષણિકતાઓનો સમન્વય કરી બનાવવામાં આવ્યો છે.

ટ્રેપડોર્સ (Trap Doors) :

ટ્રેપડોર કે બૅકડોર એ સિસ્ટમ કે તેના સ્રોતોનો અનધિકૃત રીતે ઉપયોગ કરવાનો એક વિશિષ્ટ માર્ગ છે. સિસ્ટમના વિકાસ સમયે આ માર્ગનો ઉલ્લેખ કે દસ્તાવેજીકરણ કરવામાં આવતું નથી. આ કાર્ય સામાન્ય રીતે સિસ્ટમના નિર્માતા દ્વારા પાર પાડવામાં આવે છે. જ્યારે સિસ્ટમના નિર્માતા અને સંસ્થા વચ્ચે કોઈ સંઘર્ષ થાય, ત્યારે અથવા ડેવલપર સિસ્ટમનો ગેરકાયદેસર ઉપયોગ કરવા માંગતો હોય, ત્યારે સિસ્ટમ કે કોઈ પ્રક્રિયાનો ગેરલાભ લેવા માટે આ માર્ગનો ઉપયોગ કરવામાં આવે છે.

લૉજિક બૉમ્બ (Logic Bomb) :

લૉજિક બૉમ્બ એવો પ્રોગ્રામ છે, જેનો અમલ કોઈ તાર્કિક શરત પરિપૂર્ણ થાય, ત્યારે કરવામાં આવે છે. નિશ્ચિત તારીખોની સરખામણી, કોઈ બૅન્કનાં એકાઉન્ટમાં મોટી માત્રામાં રકમ જમા કરવી અથવા તો સંસ્થાની વેબસાઇટ દ્વારા કોઈ અર્થપૂર્ણ માહિતી મેળવવી – આ કેટલીક તાર્કિક શરતોનાં ઉદાહરણ છે. જ્યારે આવી સ્થિતિ ઉદ્ભવે ત્યારે લૉજિક બૉમ્બ કેટલીક પ્રવૃત્તિઓ આચરે છે. જેમકે, અગત્યની માહિતી ચોરી લેવી, બૅન્કની સિલક બદલી નાખવી અને સિસ્ટમમાંથી અગત્યની માહિતી દૂર કરવી. સિસ્ટમના નિર્માણ સમયે નિર્માતા માટે આવા લૉજિક બૉમ્બ તૈયાર કરી સિસ્ટમ સાથે સંલગ્ન કરવા ઘણાં સરળ હોય છે.

ઉપર દર્શાવેલ તક્નિક ઉપરાંત કમ્પ્યૂટરના અનન્ય IP સરનામાંનું સ્કેનિંગ, જુદા-જુદા નેટવર્ક સ્રોત અને પોર્ટનો ઉપયોગ (સ્નીફિંગ), રી-ડાયરેક્ટિંગ, પાસવર્ડ ક્રેકિંગ, સર્વર જેવા માળખાના સેશન હાઇજેકિંગ અને સ્પૂફિંગ (DNS સ્પૂફિંગ) વગેરે પદ્ધતિઓનો ઉપયોગ કરીને સિસ્ટમનો અનધિકૃત ઉપયોગ શક્ય બનાવવામાં આવે છે. આ ઉપરાંત, હૅકરનો હેતુ સિસ્ટમના અગત્યના સ્રોતને મેળવવાનો ન હોય, પરંતુ સિસ્ટમના કાર્યને ખોરવી નાંખવાનો હોય, તો ડેનિયલ-ઑફ-સર્વિસ (denial-of-service) હુમલાઓની યોજના કરવામાં આવે છે. આ હુમલાઓ દ્વારા સિસ્ટમને બંધ કરી દેવામાં આવે છે અથવા બિનકાર્યક્ષમ બનાવી દેવામાં આવે છે. ઉપયોગકર્તાને સિસ્ટમના ઉપયોગની મંજૂરી ન આપવા દેવામાં આવતી હોવાથી તેને denial-of-service તરીકે ઓળખવામાં આવે છે. ઘણીવાર આ પ્રકારનો હુમલો કરવા સ્પામ (અનિચ્છનીય) ઈ-મેઇલનો ઉપયોગ કરવામાં આવે છે.

ઉપર્યુક્ત હુમલાઓથી સિસ્ટમ અને સ્રોતને બચાવવા માટે ઘણાં માર્ગ ઉપલબ્ધ છે. ફાયરવોલ, ઍન્ટિવાઈરસ સૉફ્ટવેર તથા અન્ય પદ્ધતિઓ દ્વારા યોગ્ય ઉપયોગકર્તાની અધિકૃતતા (જેમકે યૂઝરનેમ અને પાસવર્ડ) એ સલામતીનાં જોખમો અને વાઈરસના હુમલાઓનું ધ્યાન રાખનાર કેટલીક પ્રચલિત પદ્ધતિઓ છે. આ ઉપરાંત આ પ્રકારના હુમલાઓનો સામનો કરવા માટે સાંકેતિકરણ (સંવેદનશીલ માહિતીનું ગૂઢ લખાણમાં રૂપાંતરણ)નો ઉપયોગ પણ થઈ શકે છે, જે હવે પછીના વિભાગમાં ચર્ચવામાં આવ્યું છે.

સલામતીના સાધન તરીકે સાંકેતિકરણ (Cryptography as a Security Tool) :

ગુપ્ત (*crypto*) લખાણ (*graphy*)ની પદ્ધતિને સાંકેતિકરણ (Cryptography) કહે છે. કોઈ પણ સરળ સંદેશને ઉકેલી ન શકાય તેવા ગૂઢ સંદેશામાં પરિવર્તિત કરવો અને પુનઃ તેને સરળ સંદેશમાં પરિવર્તિત કરવો એ માટેની જુદી-જુદી તક્નિકો કે પદ્ધતિઓના વિનિયોગને સાંકેતિકરણ (Cryptrography) કહેવામાં આવે છે.

અંગતતા પૂરી પાડવા, સંચારણમાં ભાગ લેતી વ્યક્તિઓની અધિકૃતતા ચકાસવા અને સંદેશાની અખંડિતતા કાયમ રાખવા સાંકેતિકરણનો ઉપયોગ કરી શકાય છે. સાંકેતિકરણની પરિભાષા નીચે સમજાવી છે :

મૂળભૂત સાંકેતિકરણની પરિભાષા (Basic Cryptography Terminology) :

- મૂળભૂત સંદેશને સામાન્ય રીતે 'પ્લેઇન ટૅક્સ્ટ' (Plain text) કહે છે.
- ગૂઢ લખાણમાં ફેરવ્યા બાદ સંદેશને 'સાઇફર ટૅક્સ્ટ' (Cipher-text) કહે છે.
- મૂળ લખાણને ઉકેલી ન શકાય તેવા સંદેશામાં ફેરવી આપતા કોઈ તર્કને 'સાઇફર' (Cipher) કહે છે.

- પ્લેઇન ટેક્સ્ટને સાઇફર ટેક્સ્ટમાં પરિવર્તિત કરવાની ક્રિયાને 'એનસાયફરિંગ' (Enciphering) કહે છે. તેને 'એનકોડિંગ' (Encoding) કે 'એન્ક્રિપ્શન' (Encryption) તરીકે પણ ઓળખવામાં આવે છે.
- સાઇફર ટેક્સ્ટને ફરી પ્લેઇન ટેક્સ્ટમાં પરિવર્તિત કરવાની ક્રિયાને 'ડી-સાયફરિંગ' (Deciphering) કહે છે. તેને 'ડીકોડિંગ' (Encoding) કે 'ડિક્રિપ્શન' (Decryption) તરીકે પણ ઓળખવામાં આવે છે.
- ઘણીવાર સંદેશના પ્રેષક અને પ્રાપ્તકર્તા એવી મહત્ત્વની માહિતી વહેંચતા હોય છે કે જે એનકોડિંગ અને ડી-કોડિંગની પ્રક્રિયા માટે સાયફર (અલ્ગોરિધમ)ને પૂરી પાડવાની હોય છે. આ માહિતીને કી (key) તરીકે ઓળખવામાં આવે છે. કી જાહેર (Public કે Asymmetric) અથવા અંગત (Private કે Symmetric કે Secrete) હોઈ શકે છે. આ કીની ગેરહાજરીમાં સાંકેતિક લખાણ મેળવી શકાય છે, પરંતુ તેને અર્થપૂર્ણ માહિતીમાં પરિવર્તિત (Decode) કરી શકાતું નથી.
- કેટલીક વાર કીની ગેરહાજરીમાં કેટલાક લોકો સાંકેતિક લખાણને ઉકેલી તેમાંથી માહિતી મેળવવાની પદ્ધતિનો અભ્યાસ કરે છે. કીની અનુપલબ્ધતામાં સાંકેતિક લખાણને પુનઃ અર્થપૂર્ણ માહિતીમાં પરિવર્તિત કરવા માટેના સિદ્ધાંતો અને પદ્ધતિઓના અભ્યાસને Cryptanalysis કહે છે. આને 'કોડબ્રેકિંગ' (Code Breaking) પણ કહે છે.
- Cryptography અને Cryptanalysis સંયુક્તપણે Cryptology તરીકે ઓળખવામાં આવે છે.

ઉદાહરણ (Example)

સંદેશાને ઊલટસૂલટ (scramble) કરી ગૂઢ લખાણ મેળવવાની પદ્ધતિ નીચે દર્શાવેલી છે. તેના નિયમો નીચે મુજબ છે :

(1) આપેલ સંદેશાનો પ્રથમ અક્ષર તપાસો.

(2) જો એ યોગ્ય અંગ્રેજી મૂળાક્ષર હોય, તો તે અક્ષરને તેના પછીના અક્ષર પછી આવતા (next to next) પ્રમાણભૂત અંગ્રેજી મૂળાક્ષર સાથે બદલો.

(3) જો તે યોગ્ય અંગ્રેજી મૂળાક્ષર ન હોય, તો તેને પૂર્વવત્ રહેવા દો.

(4) આ ક્રિયા સંદેશના દરેક અક્ષર માટે પુનરાવર્તિત કરો.

સંદેશાને મૂળ સ્વરૂપમાં લાવવા માટે આ જ પદ્ધતિને વિપરીત ક્રમમાં અનુસરવી જરૂરી છે. ધારો કે, આપવામાં આવેલો સંદેશ છે :

My school name is New School

આ સંદેશને ગૂઢ લખાણમાં પરિવર્તિત કરવા માટેની પદ્ધતિ કોષ્ટક 14.3માં દર્શાવી છે :

Letter	M	y	Blank	s	c	h	o	o	l	Blank
Converted letter	O	a	Blank	u	e	j	q	q	n	Blank
Letter	n	a	m	e	Blank	i	s	Blank	N	e
Converted letter	p	c	o	g	Blank	k	u	Blank	P	g
Letter	w	Blank	S	c	h	o	o	l	Full stop	
Converted letter	y	Blank	U	e	j	q	q	n	Full stop	

કોષ્ટક 14.3 : સંદેશનું સાંકેતિકીકરણ

જો આપેલ પદ્ધતિને અનુસરવામાં આવે, તો સાંકેતિક લખાણ સ્વરૂપે "Oa uejqqn Pcog ku Pgy Uejqqn." ગૂઢ સંદેશ મળશે. હવે આ સાંકેતિક સંદેશને મૂળ લખાણમાં પરિવર્તિત કરવાનો પ્રયત્ન કરો.

સાંકેતિકરણ ઉપરાંત, વિગતો અને અન્ય ઘટકોને મૅમરીની બચત તથા માહિતી નેટવર્ક દ્વારા મોકલવાની હોય, તો બૅન્ડવિડ્થના હેતુથી સંકુચિત બનાવવામાં આવે છે. મૂળભૂત લખાણનો સંગ્રહ કરવા કે મોકલવાને બદલે તેની ગૂઢ તથા સંકુચિત વિગતોનો સંગ્રહ કરવામાં કે મોકલવામાં આવી શકે છે. આ અતિરિક્ત પરિશ્રમ વિગતોને મોકલવાના સમયનો, વિગતોને સંગ્રહવાની જગ્યાનો અને નેટવર્કની બૅન્ડવિડ્થનો બચાવ કરે છે. આ ઉપરાંત આ વ્યૂહરચનાને કારણે નેટવર્ક તેમજ વ્યક્તિગત કમ્પ્યૂટરને અનધિકૃત ઉપયોગથી સુરક્ષિત રાખી શકાય છે. પ્રાપ્તકર્તાના પક્ષે આ તક્નિક ડાઉનલોડ માટેનો સમય અને ખર્ચ ઘટાડે છે તથા સુરક્ષા વધારે છે. જોકે તેના માટે પ્રેષકના પક્ષે સાંકેતિકરણ અને પ્રાપ્તકર્તાને પક્ષે બિનસાંકેતિકરણ કરવા માટે થોડો વધુ પરિશ્રમ જરૂરી બને છે.

સારાંશ (Summary)

ઇન્ટરનેટ અને અન્ય નેટવર્કનો ઉપયોગ વિવિધ વિનિયોગો માટે કરી શકાય તેનો આપણે અભ્યાસ કર્યો. આ પ્રકરણમાં આપણે એક મુખ્ય વિનિયોગ ઈ-મેઇલનો અભ્યાસ પણ કર્યો. આ સાથે આપણે ઈ-મેઇલના ફાયદા, ઈ-મેઇલ ક્લાયન્ટની સંરચના અને સંદેશ મોકલવા માટેની પદ્ધતિનો અભ્યાસ કર્યો. ઇન્ટરનેટ અને વેબ એવાં માધ્યમ છે, જે સ્રોત વિતરીત કરવાની કાર્યપદ્ધતિ પૂરી પાડે છે. આવા સ્રોતની સુરક્ષાનું પૂરતું ધ્યાન રાખવું જરૂરી બને છે કારણ કે તેમની પર વાઇરસ કે કોઈ અન્ય નુકસાનકર્તા પ્રોગ્રામનું આક્રમણ થઈ શકે છે. અને પરિણામસ્વરૂપે તેમાંની માહિતી કે સ્રોતને હાનિ પહોંચી શકે છે. સાંકેતિકરણની જુદી-જુદી તક્નિકોનો ઉપયોગ કરી માહિતી કે સ્રોતને કેવી રીતે સુરક્ષિત રાખી શકાય અને અનધિકૃત ઉપયોગકર્તાના હસ્તક્ષેપથી કેવી રીતે બચી શકાય તેનો પણ આ પ્રકરણમાં આપણે અભ્યાસ કર્યો.

સ્વાધ્યાય

1. ઈ-મેઇલના ફાયદા જણાવો.
2. ઈ-મેઇલ સરનામાંનું માળખું જણાવો.
3. ઈ-મેઇલ કેવી રીતે કાર્ય કરે છે ?
4. ઈ-મેઇલનો ઉપયોગ કરી કયાં-કયાં કાર્યો કરી શકાય છે ? દરેકને એક લીટીમાં સમજાવો.
5. 'થ્રેટ' (threat) એટલે શું ? તેને કેવી રીતે દૂર કરી શકાય ?
6. નીચે આપેલ પદની વ્યાખ્યા આપો :
   - (a) ભેદ્યતા (Vulnerabilities)
   - (b) વાઇરસ (Virus)
   - (c) ટ્રોજન હૉર્સ (Trojan horse)
   - (d) વૉર્મ (Worm)
   - (e) લૉજિક બૉમ્બ (Logic bomb)
   - (f) ટ્રેપડોર (Trap door)
7. વાઇરસ અને વૉર્મ વચ્ચેનો તફાવત જણાવો.
8. 'સાઇફર' પદ સમજાવો. તે સલામતી અને સાંકેતિકરણ સાથે કેવી રીતે સંકળાયેલું છે ?

9. નીચે આપેલ પદ વ્યાખ્યાયિત કરો :

(a) ક્રિપ્ટોલૉજી (Cryptology) (b) ક્રિપ્ટાએનાલિસિસ (Cryptanalysis) (c) ક્રિપ્ટોગ્રાફી (Cryptography)

10. તમારી પસંદગીના કોઈ પણ ત્રણ ઈ-મેઈલ ક્લાયન્ટની યાદી બનાવો.

11. **આપેલ વિકલ્પોમાંથી યોગ્ય વિકલ્પ પસંદ કરો :**

(1) ઈ-મેઈલ દ્વારા કયા પ્રકારની માહિતી મોકલી શકાય છે ?

(a) લખાણ અને ધ્વનિ (b) લખાણ અને અંકો

(c) મલ્ટિમીડિયા (d) આપેલ તમામ

(2) જન્કમેઈલને અન્ય કયા નામથી ઓળખવામાં આવે છે ?

(a) ઓછા મહત્ત્વના મેઈલ (b) અતિ મહત્ત્વના ઝડપી મેઈલ

(c) બિનજરૂરી મેઈલ (d) આપેલ તમામ

(3) ઈ-મેઈલ મોકલવા માટે કમ્પ્યૂટર અને મૂળભૂત ઈન્ટરનેટની સુવિધા ઉપરાંત નીચેનામાંથી શેની જરૂર પડે છે ?

(a) ઈ-મેઈલ આઈ-ડી કે ઈ-મેઈલ સરનામું (b) સ્થાયી સરનામું

(c) ટપાલ-સરનામું (d) આપેલ તમામ

(4) સૉફ્ટવેર સાથે આવતા અને સિસ્ટમને નુકસાનકર્તા પરોપજીવી પ્રોગ્રામને કયા નામથી ઓળખવામાં આવે છે ?

(a) હુમલો (Attack) (b) વાઈરસ (Virus)

(c) ભેદ્યતા (Vulnerabilities) (d) આપેલ તમામ

(5) કોઈ તર્કનો ઉપયોગ કરીને મૂળ સંદેશને ઉકેલી ન શકાય, તેવા સ્વરૂપમાં ફેરવવા માટે નીચેનામાંથી શેનો ઉપયોગ કરવામાં આવે છે ?

(a) કાઈસન (kaison) (b) સાઈફર (cipher)

(c) લૉજિક બૉમ્બ (logic bomb) (d) ઍટમ બૉમ્બ (atom bomb)

(6) નીચેનામાંથી કયા વિનિયોગ દ્વારા વિવિધ તક્નિકો અને સિદ્ધાંતોનો ઉપયોગ કરી સામાન્ય લખાણને ઉકેલી ન શકાય તેવા સ્વરૂપમાં ફેરવવા તથા ફરી તેને મૂળભૂત સ્વરૂપમાં લાવવા માટેની રીતોનો ઉપયોગ કરી શકાય છે ?

(a) ક્રિપ્ટોગ્રાફી (Cryptography) (b) ક્રિપ્ટોએનાલિસિસ (Cryptanalysis)

(c) ક્રિપ્ટોલૉજી (Cryptology) (d) આપેલ તમામ

(7) ગૂઢ લખાણને મૂળ સંદેશમાં ફેરવવાની ક્રિયાને કયા નામથી ઓળખવામાં આવે છે ?

(a) Enciphering (b) Encryption

(c) Deciphering (d) Decryption

(8) ક્રિપ્ટોએનાલિસિસ (Cryptanalysis)ને અન્ય કયા નામથી ઓળખવામાં આવે છે ?

(a) કોડ બ્રેકિંગ (b) લૉજિક બ્રેકિંગ

(c) ડિઝાઈન બ્રેકિંગ (d) સિસ્ટમ બ્રેકિંગ

(9) ક્રિપ્ટોગ્રાફી (cryptography) અને ક્રિપ્ટોએનાલિસિસ (cryptanalysis)ને કયા સંયુક્ત નામથી ઓળખવામાં આવે છે ?

(a) ક્રિપ્ટોગ્રાફી (b) ક્રિપ્ટોએનાલિસિસ

(c) ક્રિપ્ટોલૉજી (d) આપેલ તમામ

પ્રાયોગિક સ્વાધ્યાય

1. તમારું ઈ-મેઈલ એકાઉન્ટ બનાવી તમારા મિત્રને સંદેશ મોકલો. તમારા મિત્રને તેનો જવાબ આપવાનું જણાવો.
2. મિત્રના સંદેશની પ્રતિક્રિયા આપતો ઈ-મેઈલ કોઈ બિડાણ સાથે મોકલો.
3. એકથી વધુ મિત્રોને સંદેશ મોકલો.
4. તમારી પસંદગીના કોઈ સંદેશનું સાંકેતિકીકરણ કરો. તેને ટાઈપ કરી ઈ-મેઈલ દ્વારા તમારા મિત્રને મોકલો. તમારા મિત્રને સંદેશનું બિનસાંકેતિકીકરણ કરવા કહો.
5. તમારા કમ્પ્યૂટરમાં આવેલ ઍન્ટિવાઈરસ પ્રોગ્રામ ચલાવી વાઈરસની શોધ કરો.

◆