ሴፍ ሲስትርስ (Safe Sisters)

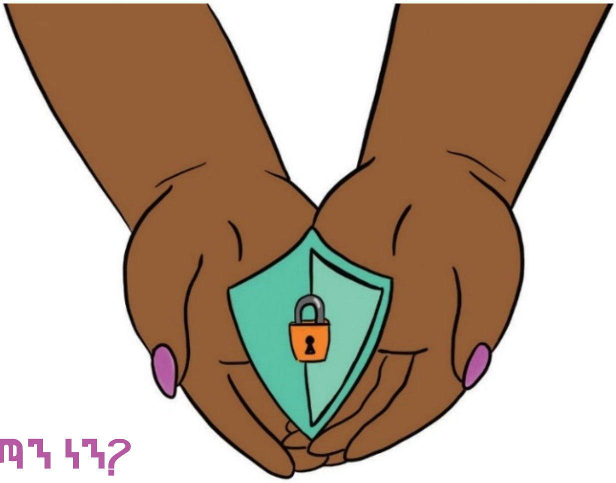
በ አፍሪካ ከሰሀራ በታች ለሚኖሩ ሴቶች እና ልጃገረዶች የተዘጋጀ የዲጂታል ደህንነት መተግበሪያ ቀላል መመሪያ

ለማውረድ እና የበለጠ ለመረዳት https://safesisters.net ላይ ይመልከቱ።

አማርኛ

ይህ መርጃ መፅሀፍ ምንድን ነው?

ይህንን መመሪያ ለማንበብ ስላነሱት እናመሰግናለን። ይህ መመሪያ የተዘጋጀው ሴቶች በይነመረብን (ኢንተርኔት) ሲጠቀሙ የሚደርስባቸውን ችግር (ለምሳሌ የተለቀቁ ወይም የተሰረቁ ፎቶዎች፣ ቫይረሶች እና የማጭበርበሪያ መልዕክቶች (ስካሞች) እና የመሳሰሉትን እንዲገነዘቡት ለማስተማር ነው። ከነዚህ በይነመረብን (ኢንተርኔትን) ተመስርተው ከሚፈፀሙ ጥቃቶች ራሳችንን ለመጠበቅ የሚያስችለንን ትክክለኛውን ውሳኔ እንዴት እንወስናለን? እንዲሁም ኢንተርኔትን ለግል ጥቅማችን፣ ለቤተሰቦቻችን ብሎም ለሁሉም ሴቶች ከጥቃት የተጠበቀ ቦታ እንዴት ማድረግ እንችላለን? የሚለውን ጠቅለል ያለ ምላሽ ለመስጠት ታስቦ የተዘጋጀ መመሪያ ነው።



እኛ ማን ነን?

ይህ መመሪያ በ Internews; Defend Defenders እና በ 2018-2019 Safe Sister fellowship program የጋራ ትብብር የተዘጋጀ ነው። ይሄንን መመሪያ የሁለተኛ ዙር የሴፍሲስተርስ ፌሎዎች የሆኑት ሀና አስማረ፣ ሀይማኖት ተፈራ፣ ነፃነት ሙሉነህ፣ እና ሰላማዊት ተዘራ ወደ አማርኛ ቋንቋ ተርጉመውታል። ተልእኳችንም የዲጂታል ደህንነትን ውስብስብነት በመቀነስ ለትክክለኛ ተጠቃሚዎቹ ይበልጥ አግባብነት እንዲኖረው በማስቻል ሴቶች እና ልጃገረዶች ለደህንነታቸው ዘብ እንዲቆሙ ማበረታታት ነው። የዚህ መመሪያ አንባቢዎች በይነመረብን በሚጠቀሙበት ወቅት እራስን ለመጠበቅ በዕለት ተዕለት ህይወት የምንጠቀምባቸው የተለመዱ የግንዛቤ ስልቶች ጭምር ውጤታማ የሆኑ መንገዶች መሆናቸውን እንደሚረዱ ተስፋ እናደርጋለን።

አላማችን

- የዲጂታል ቴክኖሎጂን በአግባቡ ስራ ላይ ለማዋልና ውስብስብነቱን ለመቀነስ፤
- ልንጠቀም ከምንፈልገው ነገር ጋር አግባብነት ያለው ግንኙነትን መፍጠር፤
- ሁሉም የበይነመረብ ተጠቃሚ ሴቶች ኦንላይን ላይ የሚኖራቸውን ጊዜ ከአደጋ የተጠበቀ ማድረግ፤
- ከአደጋ የተጠበቀ አጠቃቀምን እያሳወቁ እንዲጠቀሙበት ማበረታታት።

A program by: Graphics by:

Internews DEFENDDEFENDERS East and Horn of Africa Human Rights Defenders Project POLLICY

አይሻን እንተዋወቅ!

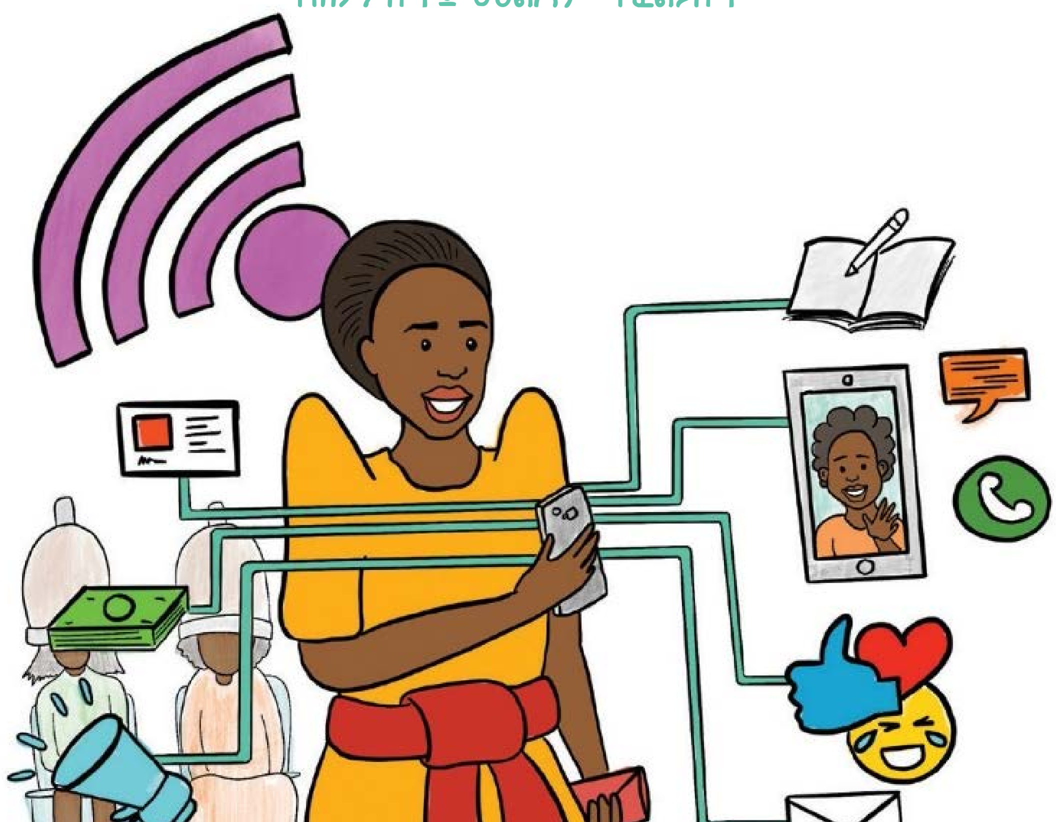
አይሻ አዲስ አበባ፣ ኢትዮጵያ ውስጥ የምትኖር ወጣት ሴት ነች፡፡ እሷ እና ጓደኞቿ አዘውትረው በይነመረብን (ኢንተርኔት) ይጠቀማሉ፤ ድህረ ገፆችን ይጎበኛሉ፤ በፌስቡክ ገፃቸው ላይ አዳዲስ ነገሮችን ይለጥፋሉ፤ ኢንስተግራም ላይ ፎቶ ይጭናሉ፤ በትዊተር ሀሳብ ይለዋወጣሉ፤ በቫይበር እና ዋትስአፕ ከጓደኞቻቸው እና ቤተሰቦቻቸው ጋር የፅሁፍ መልእክት ይላላካሉ፤ ጉግልን በመጠቀም ነገሮችን ያፈልጋሉ፤ እንዲሁም ለስራቸው ኢሜል ይላላካሉ፡፡

አይሻ እናቷ፤ አባቷ እና ታናሽ እህቷ ማርያም ከሚኖሩበት መንገድ በታች፣ ከታዳጊ ሴት ልጇ ከናቱ ጋር አብራ ትኖራለች፡፡ አይሻ የማህበራዊ ድህረገፅ አካውንታቸው ሀክ የተደረገባቸው (በሌላ አካል የተጠለፈባቸው) እና እነርሱ ሳያውቁት ፎቶዋቸው የተለጠፈባቸው ጓደኞች አሏት፡፡ በዚህም ምክንያት ስለቤተሰቦቿ እና ስለራሷ ደህንነት ታስባለች፡፡

በዚህ መመሪያ ውሰጥ አይሻ በይነመረብን ወይም የማህበራዊ ትስስር አውታሮችን ስትጠቀም የምታስገባው መረጃ ላይ ስለሚደርሰው ነገር ትጠይቃለች፤ ኦንላይን ስትሆን በጥንቃቄ የመጠቀሚያ መንገዶችን ታገኛለች፤ እንዲሁም ጓደኞችዋን እና ሴት ልጇን በጥንቃቄ እንዲጠቀሙ ታስተምራለች፡፡

112

አይሻ ስለዲጂታል ደህንነት ለማወቅ የተለያዩ ጥያቄዎች ትጠይቃለች፤ መልስም ትፈልጋለች



የአይሻ ጥያቄ

አንድ ሰው የኔን አካውንት ሀክ ማድረግ (ካለ እኔ እውቅና አካውንቴን ሊጠቀምበት) ይችላል?

የአይሻ የአጎት ልጅ የሆነቸው ራሄል የፌስቡክ አካውንት በባለፈው አመት በሌላ ሰው ሀክ ተደርጎ (ከእሷ እውቅና ውጪ ተጠልፎ) እሷ ያልፃፈቸው ነገር በገጿ ላይ ተለጥፏል፡፡ ራሄል ለፌስቡክ የተፈጠረውን ነገር አሳውቃለች፡፡ እነሱም አካውንቷን መልሳ እንድትቆጣጠር የረዷት ቢሆንም ሀክ እንዴት ልትደረግ እንደቻለች ማወቅ አልቻለችም፡፡

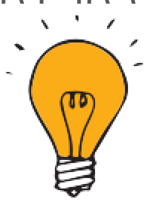
የራሄል አካውንት ውስጥ አንድ ሰው በተለያየ መንገድ ሊገባ ይችላል፡፡ የይለፍ ቃሏን (password) ያወቀ ሰውም ሊሆን ይችላል፡፡ ብዙ ሰዎች የሰዎችን የይለፍ ቃል ይሰርቃሉ፡፡ ይህ ልክ እንደ ንግድ እየተስፋፋ ያለ ነገር ነው፡፡

የይለፍ ቃልዎ ለሀከሮች (ለጠላፊዎች) አስፈላጊ ነው ምክንያቱም ስለእርሶ ያለውን መረጃ ለነሱ የመክፈቻ ቁልፍ ነው፡፡ ለምንድን ነው የሚሳካላቸው? አንደኛው ምክንያት የምንጠቀማቸው የይለፍ ቃላቶች በቀላሉ በሌሎች መገመት ወይም ሊሰበሩ በመቻላቸው፤ በኮምፕዩተራችን መሰረቅ እና በወንጀለኞች ጥቅም ላይ መዋላቸው ነው፡፡

1/3

በእንግሊዘኛ ቋንቋ p@ssw0rd የተለመደና በብዛት ጥቅም ላይ የሚውል የይለፍ ቃል እንደሆነ ታውቃላችሁ?

ለተሻለ የይለፍ ቃል ይሄንን መንገድ ተጠቀሙ፤



- ጠንካራ የይለፍ ቃል መጠቀም ከሀከሮች (ከጠላፊዎች) እራስን የመከላከያው የመጀመሪያው መንገድ ነው፡፡ ስለዚህም የይለፍ ቃልን ስንመርጥ በብልሀት ይሁን፡፡
- ለተለያየ የማህራዊ ድህረ-ገፅ አካውንት የተለያየ የይለፍ ቃል መጠቀም ይመረጣል፡፡ አንድ የይለፍ ቃል ለሁሉም የማህራዊ ድህረ-ገፅ አካውንት መጠቀም ጠላፊዎች (ሃከሮች) በቀላሉ ሁሉንም የማህራዊ ድህረ-ገፆች ሠብረው እንዲገቡ እድል ይሠጣቸዋል፡፡
- የምትጠቀሟቸውን ሁሉንም የይለፍ ቃላት ለማስታወስ የምትቸገሩ ከሆነ password manager (የይለፍ ቃል አስተካካይን) ለመጠቀም ይሞክሩ፡፡ እናንተ ማስታወስ ሳይጠበቅባችሁ እራሱ ያላችሁን የይለፍ ቃላት በሙሉ ያስታውስላችኋል፡፡ እናም እናንተ ማስታወስ ያለባችሁ ነገር ቢኖር ዋናውን የይለፍ ቃል (master password) ነው፡፡

የአይሻ ጥያቄ

ጠንካራ የይለፍ ቃል እንዲኖረኝ እንዴት ማድረግ እችላለሁ?

አካዉንታችንን ከሀከሮች (ከጠላፊዎች) ለመጠበቅ ትንሽ ጥረት ማድረግ ብዙ ልዩነት ሊያመጣ ይችላል፡፡የተለመደ የይለፍ ቃል መጠቀም አሁን አሳሳቢ እየሆነ የመጣ ነገር ነው፤ ምክንያቱም የተለመደው አይነት የይለፍ ቃል በብዛት አጭርና ቀላል በመሆኑ የኮምፒውተር ሀከሮች በቀላሉ ሊሰብሩት ወይም ሊገምቱት ይችላሉ፡፡

በዚህ ፋንታ ጅምር አረፍተ ነገር (passphrase) ለመጠቀም ሞክሩ፡፡ ጅምር አረፍተ ነገር (passphrase) በብዙ ቃላት ጥምረት የሚዘጋጅ የይለፍ ቃል አይነት ነው፡፡ አንድን ቃል ከማስታወስ የበለጠ ለማስታወስ ቀላል እና ጠንካራ ነው፡፡ በተለይም ረዥም የሆኑት ጅምር አረፍተ ነገሮች (passphrase) ይበልጥ አቅማቸው በተሻሻሉት ኮምፕዩተሮች እንኳን በቀላሉ ሊሰበሩ አይችሉም፡፡

የአይሻ የፌስቡክ የይለፍ ቃል **@ugust2013** ሲሆን ታናሽ እህቷ የተወለደችበትን ወርና አመትን የያዘ ነው፡፡ ይህንን የይለፍ ቃል ለመገመት በተለይም እህቷን ማወቅ ለቻለ ሰው በጣም ቀላል ነው፡፡ አይሻ ጅምር አረፍተ ነገሯ (passphrase) ጠንካራ እንዲሆን ወደ Ey3L1K3MyFr13nds&Fam1ly! ቀይራዋለች (ይሄም ለአይሻ "ጓደኞቼን እና ቤተሰቦቼን እወዳለሁ") እንደማለት ነው፡፡

//4

ለጠንካራ የይለፍ ቃል ይሄንን መንገድ ተጠቀሙ፤

- የይለፍ ቃሉ ረዥም ቢሆን የተሻለ ነው! እንዲሁም በተቻላቹት መጠን የምትጠቀሙት የይለፍ ቃል ከ15 ፊደል በላይ የያዘ እና ምልክት (@፣ %፣ &፣ #)፣ ቁጥሮችን (1፣2.3…) እና የእንግሊዘኛ ትልቁን እና ትንሹን ፊደላት ያካተተ (A,a,B,b..) እንዲሆን አድርጉ፡፡
- ጠንካራ ጅምር አረፍተ ነገር (passphrase) መጠቀም በራሱ ሁሌም በቂ ላይሆን ይችላል፡፡ በጣም አስፈላጊ የሆኑ አካውንቶችዎ የበለጠ ደህንነት እንዲኖረቸው ከፈለጉ ባለ-ሁለት እርከን ማረጋገጫ (Two Factor Authentication 2FA) ተጠቀሙ፡፡ አብዛኞቹ ታዋቂ የሆኑ የማህበራዊ ትስስር ድህረ ገጾች፣ ለምሳሌ እንደ ፌስቡክ፣ ጂሜይል፣ ትዊተር፣ ኢንስተግራም ያሉት ባለ-ሁለት እርከን መተግበርያ (2FA) ወደ አካውንታችሁ ለመግባት እንደ ተጨማሪ አማራጭ ያቀርባሉ፡፡
- አንድን የይለፍ ቃል ወይም ጅምር አረፍተ ነገር (passphrase) መጠቀም ያለባችሁ ለአንድ አካውንት ብቻ መሆን አለበት፡፡ ምክንያቱም አንድ ሰው የይለፍ ቃል ወይም ጅምር አረፍተ ነገሩን ካወቀው በቀላሉ ወደ ሌላኛው አካውንታችሁ መግባት ወይም መጠቀም ይችላል፡፡

የአይሻ ጥያቄ

የማህበራዊ ትስስር ድህረ ገፅ ላይ ምንድነው መለጠፍ ያለብኝ?

እንደ አብዛኛው ሰው ተጠቃሚ ከሆናችሁ ማህበራዊ ትስስር ድህረ ገፅ ከሰዎች ጋር ለመግባባት እንዲሁም ከቤተሰብና ከጓደኞች ጋር ለመገናኘት አመቺ መንገድ ነው፡፡

ሰዎች ራሳቸውን የሚመለከቱ የተለያዩ መረጃዎችን በእነዚህ ገጾች ላይ ይለጥፋሉ፤ እንዲሁም ይልካሉ፡፡ ነገር ግን የማያስተውሉት ነገር ቢኖር እነሱን የማያውቁ ሰዎች ፎቶዎቻችን እና አስተያየቶቻችን (comments) ሊያዩ እንደሚችሉ ነው፡፡ በተጨማሪም እነሱን የማያውቁ ሰዎች የፌስቡክ ገፃቸውን በመመልከት ስለነሱ ብዙ ነገሮችን ሊያውቁ ወይም ሊያገኙ ይችላሉ፡፡

ስለሆነም ምን አይነት መልዕክት፣ ቪድዮ እና ምስሎችን በማህበራዊ ድህረ-ገፅ ላይ ማጋራት እንዳለባችሁ በአግባቡ መምረጥ አለባችሁ፡፡

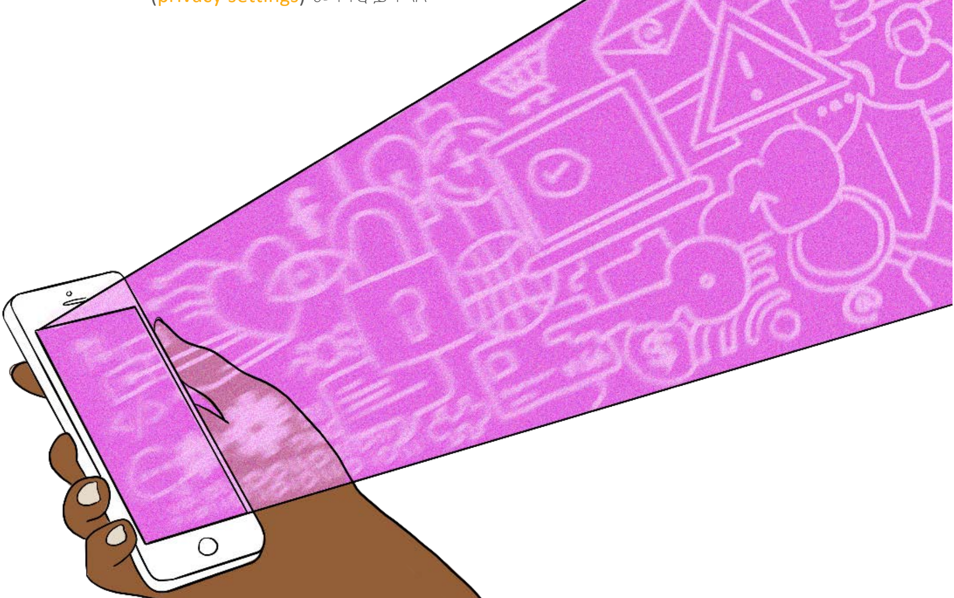
አስታውሱ፡

በማህበራዊ ድህረ - ገፅ ላይ የምታጋሩት መረጃ መቼም የሚጠፋ አይደለም

ይሄንን መንገድ ተጠቀሙ፤

//5

- ጉግል ላይ ስምዎትን አስገብተው በመፈለግ ስለ እርሶ ምን ያህል መረጃ ሌላ ሰው ሊያገኝ እንደሚችል ይመልከቱ፡፡
- የእርስዎ የቅርብ ሰው የማህበራዊ መገናኛ ትስስር መረጃዎትን በማየት ሰለእርስዎ ግላዊ መረጃ ምን ያህል ማወቅ ይችላል? ስለ እርስዎ ያለውን ግላዊ መረጃ ህዝቡ ቢያውቀው ደስተኛ ኖት? ደስተኛ ካልሆኑ አካውንትዎ ላይ ያለውን የግል መተግበሪያ (privacy settings) መቀየር ይችላሉ፡፡



የአይሻ ጥያቄ

አንድ ሰው የይለፍ ቃሌን ሳይጠቀም ወደአካውንቴ ሊገባ ይችላልን?

ከማታውቋቸው ሰዎች ድንገተኛ ሊንኮች ወይም "ሽልማት በማሸነፎ እንኳን ደስ አለዎት" የሚል መልዕክት ደርሶት ያውቃል? ምን አልባት ደግሞ ኮምፒውተርዎ በቫይረስ ስለተጠቃ አዘምኑት (አፕዴት) አድርጉ የሚል መልዕክት ይደርስዎታል?

የይለፍ ቃልዎን ከመስበር በተጨማሪ ሰዎች ከእርስዎ ፍቃድ ውጪ ቫይረስ (malware) በመላክ ወደ አካውንትዎ መግባት ይችላሉ። እነዚህ ቫይረሶች ጎጂ የኮምፒውተር ፕሮግራሞች ሲሆኑ ኮምፒውተርዎ ወይም አካውንትዎ ላይ ያሉ መረጃዎችን በቀላሉ መዝረፍ ከመቻላቸው በተጨማሪም ማንነትዎን እና የሂሳብ መረጃዎችዎን ለመስረቅ ያስችላሉ። ይሄንን የዝርፊያ መንገድ የሚያመቻቹላቸው ሳያውቁት የሚላክልዎትን የተሳሳቱ ሊንኮች በመክፈት፣ malware (የኮምፒውተር ቫይረስ) ያለበትን የማይታመን ፋይል በመጫን (ዳውንሎድ ሲያደርጉ) ወይም ሲከፍቱ ቫይረስ ወደ ኮምፒውተርዎ ይገባል።

116

ራስዎን ከአካውንት ዝርፍያ ለመጠበቅ ይሄንን መንገድ ተጠቀሙ፤

- በማታውቋቸው ሰዎች የሚላኩ የኢ-ሜይል አባሪ ሰነዶችን (አታችመንቶችን) እና ሊንኮችን ተጠራጠሩ እንዲሁም ትኩረት ስጡ። የላኪውን መረጃ በደንብ አድርገው ያጢኑ እናም ልክ የማይመስል ነገር ከተመለከቱ መልእክቱን ወይም ሊንኩን አይጫኑ።
- ስልክዎ ወይም ኮምፒውተርዎ ቫይረስ ስላለበት አዘምኑ (አፕዴት) ወይም ያውርዱ (ዳውንሎድ) አድርጉ" የሚል የማስጠንቀቂያ መልእክት ከመጣልዎት፤ ተጠንቀቁ!! ምክንያቱም እውነተኛ ላይሆን ስለሚችል። በደንብ አጢናችሁ ተመልከቱት፤ ትክክለኛ ይመስላል? እርግጠኛ ካልሆናችሁ የማስጠንቀቂያ መልእክቱን በይነ መረብ ላይ (ጉግል ላይ ፃፉና ሌላ ሰው ይህንኑ ሪፖርት እንዳደረገ ተመልከቱ።
- ሶፍትዌር ማዘመኛ (software update) እንድታደርጉ የሚመጣላችሁን መልእክት ችላ አትበሉ። ሶፍትዌር ማዘመኛ አስፈላጊ የሆነው አዳዲስ ነገሮችን እና ኮምፕዩተራችንን ከቫይረስ የሚከላከሉ የጥንቃቄ ማዘመኛዎች (security updates) ይዘው ስለሚመጡ ነው። ይህንን ለማድረግ ከፈለጋችሁ በቀጥታ የሶፍትዌር ዌብሳይት ላይ በመሄድ ከዛው ላይ ጫኑ (ዳውንሎድ አድርጉ)።

የአይሻ ጥያቄ

በይነ መረብ ስጠቀም (ኦንላይን) የማደርገውን ነገር ሌላ ሰው ያየኛልን?

ኦንላይን ስትሆኑ ሌላ ሰው ያየኛል ብሎ ማሰብ የተለመደ ነው።ይህ ማለት ሌላ ሰው የናንተን ቪዲዮ እያየ ነው ማለት አይደለም። ነገር ግን አብዛኛውን ጊዜ ድህረገፅ ስትጠቀሙ፤ ዌብሳይት በምትጎበኙበት እና የተለያዩ መተግበሪያዎች(አፕልኬሽኖች) በምትጠቀሙበት ጊዜ የዲጂታል አሻራ ወይም መረጃ ትተዋላችሁ። የምትወዱት ወይም የምትጠሉት ምን እንደሆነ፣ የጓደኞቻችሁን ስም፣ የምትማሩበት ትምህርት ቤት፣ የፖለቲካ አስተያየታችሁን፣ ከዛም አለፍ ሲል ባለፈው ሳምንት የበላችሁትን እራት እንኳ ሳይቀር ታጋራላችሁ። በዚህም መረጃዎችን ልትተው ትችላላችሁ።

//7

አብዛኞቹ በእለተ ተእለት የምንጠቀማቸው ዌብሳይቶች ከኛ መረጃ በመሰብሰብ ለአስተዋዋቂዎች በሚሸጡ የመረጃ ነጋዴዎች ባለቤትነት ስር የሚተዳደሩ ናቸው። የዲጂታል አሻራዎቻችሁ በነዚህ ድርጅቶች በአሁኑ ሰአት ሊሰበሰብ ይችላል።ኦንላይን በምትሆኑበት ጊዜ የግል መረጃችሁን በተሻለ ሁኔታ ለመጠበቅ እና ትንሽ መረጃ ለመተው የተለያዩ መንገዶችን መጠቀም ትችላላችሁ።

ለምሳሌ፤

- አንድ መተግበሪያ (አፕልኬሽን) በነፃ የምንጠቀም ከሆነ መተግበሪያውን የሰራው ሰው (የአፕልኬሽን ዴቨሎፐር) ገንዘብ እንዴት የሚያገኝ ይመስችኋል? አብዛኛውን ጊዜ ገንዘብ የሚያገኘው ከኛ የሚገኘውን መረጃ በመሰብሰብ ለተለያየ ምርት ሻጮች እና አስተዋዋቂዎች በመሸጥ ነው።
- ሁሌም ለውጥ (ማዘመኛ) ስለሚደረግባቸው የምትጠቀሟቸውን የማህበራዊ ድህረገፆች የግል መተግበሪያ (privacy setting) ፈትሹ።
- በስልካችሁ ላይ የመተግበሪያ ፈቃድ (app permissions) ወደሚለው በመሄድ የምትጠቀሟቸውን መተግበሪያዎች (አፕልኬሽኖች) ከእናንተ ምን መጠቀም እንደሚችሉ ተመልከቱ። ስልካችሁ ላይ ያሉ የስልክ ቁጥር አድራሻዎች (contacts)፣ የድምፅ ማስተላለፊያ (microphone)፣ መገኛችሁን (location) መጠቀም የሚችሉ መተግበሪያዎች (አፕልኬሽኖችን) ተጠንቀቁ፤ እናም የመተግበሪያ ፈቃድ (app permissions) የሚለው ላይ በመሄድ ስትፈልጉ ለውጥ አድርጉ።

የአይሻ ጥያቄ

ከሌላ ስልክ ወይም ኮምፕዩተር ከመሳሰሉት መጠቀሚያዎች (devices) ጋር ከተገናኘው ምን ማድረግ አለብኝ?

በሥራ፣ በቤት ወይም ኢንተርኔት ካፌ ውስጥ ከሌሎች ኮምፕዩተሮች ጋር የተገናኘ ኮምፒውተር የሚጠቀሙ ከሆነ ሌሎች የሚጠቀሙት ሰዎች በቀላሉ የሰሩትን ማንኛውንም ነገር፣ የጎበኙትን ድህረ-ገጽ ጨምሮ የእርስዎን የግል መልእክቶች፣ ኢ-ሜሎች፣ የእርስዎን ፎቶዎች፣ ያጋሯቸውን ቪዲዮዎች ወይም አካውንትዎ ላይ ያደረጉትን ማሻሻያ (update) መመልከት ይችላሉ።

ሰዎች የእርስዎን መረጃዎች የመጠቀም እድል እንዳይኖራቸው ለማረጋገጥ ተመራጭ የሚሆኑት መንገዶች ኮምፒውተርዎን ተጠቅመው ሲጨርሱ ከመውጣትዎ በፊት የጉብኝት ታሪክ (browser history) ማጥፋት፣ ማንኛውም አካውንትዎን (እንደ ኢ-ሜይል ወይም ማህበራዊ ድህረ ገጽ ያሉትን) በአግባቡ ዘግቶ መውጣት (sign out ማድረግ) እናም ከተቻለ ከኮምፒውተርዎ በአግባቡ ዘግቶ መውጣት (log out) ማድረግ ናቸው።

118

ሰዎች የእርስዎን የግል መረጃዎች እያነበቡ ወይም የእርስዎን ፎቶዎች እያዩ አስቸግረዎት ከሆነ ወደ ኮምፒውተርዎ አያውርዱ (download) አያድርጉት። በሱ ፋንታ ጎግል ድራይቭ (Google Drive) ወይም ድሮፕ ቦክስ (Dropbox) የሚባሉ የበይነ መረብ ማስቀመጫዎችን (cloud storage) አማራጮች ላይ አስቀምጧቸው። ነገር ግን ከመውጣትዎ በፊት በአግባቡ ዘግቶ መውጣት (sign out ማድረግዎን) ያረጋግጡ።

የእርስዎን ኮምፒውተር ወይም ስልክ የቤተሰብ አባልዎት የሚጋራዎት ቢሆን እንኳ ሁልጊዜ የይለፍቃል ወይም የይለፍ ቁጥር (pin code) መጠቀም ወሳኝ ነው።ይህን ማድረግዎ ስልክዎ ወይም ኮምፕዩተርዎ ቢሰረቅ እንኳ የሰረቀው ሌባ የእርስዎን ጠቃሚ መረጃ እና ፎቶዎች ለመጠቀም እድል እንዳይኖረው ያደርጋል።

አስተዉሉ፤

- ኮምፒውተርዎን ከማያምኑት ሰው ጋር የሚጋሩ ከሆነ አነዚህ ሰዎች በኮምዩተርዎ ላይ እርስዎ የሚሰሩትን ለመከታተል የሚያስችል ሶፍተዌር ሊጭኑበት ይችላሉ። ይህ ሶፍትዌር በተለምዶ ስፓይዌር (spyware) ይባላል። ስፓይዌር ያለበት ኮምፕዩተር እየተጠቀሙ እንደሆነ ካሰቡ ኮምፕዩተርዎ ላይ ስለሚሰሩት ነገር ይጠንቀቁ።
- አንድ የምታውቁት ሰው በስልክዎ ላይ የሚገኘውን የግል መልእክቶች ከፍቶ ለማንበብ የፈለገ እንደሆነ ሌላ ሰው እንዳያየው የማይፈልጉትን አደጋ ላይ የሚጥልዎትን መረጃ ማጥፋትዎን ያረጋግጡ።

የዲጂታል ደህንነት በቁጥር ሲቀመጥ

ዲጂታል ደህንነትን በሚመለከት ብዙ እውቀት የለኝም ብለው የሚያስቡ ከሆነ ብቻዎትን አይደሉም፡፡

ይህንን መምሪያ ለማዘጋጀት 500 በሚሆኑ ሴቶች ላይ የዲጂታል ደህንነት ላይ ያላቸውን እውቀት እና ልምድ ለማወቅ በ2012 ዓ.ም ጥቅምት ወር ላይ በአዲስ አበባ፣ ኢትዮጵያ ጥናት አካሂደን ይህንን ማወቅ ችለናል፡፡

መረጃ መረብ ላይ ትንኮሳ አጋጥሞት ወይም ደርሶብዎት ያውቃል?

አይ (68%) አዎ (32%)

አፕሊኬሽኖችን፣ ሊንኮችን፣ የኮምፒውተር ኦፕሬቲንግ ሲስተሞችን እና ሶፍትዌሮችን በየጊዜው አዘምናለሁ።

አይ (51%) አዎ (49%)

በጣም ጠቃሚ ለሆኑ ኦንላይን መለያዎቼ ባለ ሁለት ማረጋገጫ ያለውን መጠበቂያ (2 ኤፍ ኤ) እጠቀማለሁ።

አይ (29%) አዎ (12%)

ስለ 2ኤፍኤ ግንዛቤ የለኝም (59%)

አይሻ የምታደርጋቸው ለውጦች ዝርዝር

አሁን አይሻ ስለዲጂታል ደህንነት በብዙ ስላወቀች፤ ኦንላይን ስትሆን እራስዋን ለመጠበቅ የምታደርጋቸውን ለውጦች እንመልከት፡፡

1 የተሻለ የይለፍ ቃል መጠቀም

ጠንካራ ጅምር አረፍተ ነገር (passphrase) አዝናኝ በማድረግ የምትወደውን የዘፈን ግጥም፣ የተለያዩ ፊደላትን፣ ቁጥሮችን እና ትልቅ እና ትንሽ በማቀላቀል መፍጠር፣ እንዲሁም ለሁሉም አካውንቶች ተመሳሳይ የይለፍቃል ከመጠቀም መቆጠብ፡፡

2 ከመጫኗ በፊት ቀድማ ማሰብ

ከዚህ ሰአት በኋላ አጠራጣሪ ሊንኮች እና አባሪ ሰነዶች (አታችመንቶችን) አትጫኔንም (ክሊክ አታደርግም)፤ እንዲሁም የላኪውን መረጃ እና የኢሜሉን ይዘት በደንብ በማጤን ከማታውቃቸው ሰዎች የሚላኩ ኢሜሎችን በጥርጣሬ ታረጋግጣለች፡፡

3 ሁሌም በአግባቡ ዘግቶ መውጣትን(log off) ማድረግዋን ማስታወስ

በስልክ እና ኮምፒውተሯ ላይ ያለውን የጥንቃቄ መተግበሪያ (security setting) መመልከት፤ ወደ ኮምፒውተር ወይም ስልኳ ለመግባት የይለፍ ቃል እንዲኖረው መጨመር፤ እና ከሌሎች ጋር የምትጋራውን ኮምፒውተር ወይም ስልክ ተጠቅማ ስትጨርስ ከአካውንቷ በአግባቡ ዘግታ መውጣት (signout) ማድረግ፡፡

4 በበይነ መረብ ላይ ስለምታጋራው መረጃ እና ስለምታደርገው ነገር መጠንቀቅ

በድህረገፅ የተለቀቀ ፎቶ ወይም ፅሁፍ አንዴ ካጋሩት መልሶ ለማስወገድ አይቻልም ማለት ይቻላል፡፡ ስለዚህም በማህበራዊ ድህረገፅ ላይ ከማጋራት በፊት በጥንቃቄ ማሰብ ይኖርባታል፡፡ የማህበራዊ ድህረገፅ መተግበሪያዎችን የግል መተግበሪያ (privacy setting) በደንብ መመልከት እና አስፈላጊውን ለውጥ ማድረግ፤ በተጨማሪም መተግበሪያዎችን (አፕልኬሽኖቹ) የምትሰጠውን ፍቃድ (app permissions) (ቦታ፣ የድምፅ ማስተላለፊያ፣ የአድራሻ ዝርዝር) እና የምትሰሩትን ነገር ማየት የሚችሉትን ሰዎች መገደብ፡፡

5 ለሴት እህቶቿ ደራሽ መሆን

የግል (ወጣ ያለ ይዘት ያላቸው ፎቶዎች) በማህበራዊ ድህረ-ገፅ መለቀቃቸው በተለይም ሴቶች ላይ ትልቅ ጉዳት ያደርሳል፡፡ የሴት እህቶቻችንን የግል (ወጣ ያለ ይዘት ያላቸው ፎቶዎች) ለሌሎች ሰዎች መላክ የለብንም፤ እንዲሁም ሴት እህቶቻችን በዚህ ችግር ላይ ሲወድቁ ድጋፍ ማድረግ ያስፈልጋል፡፡ ሌሎች በበይነ መረብ ተጠቅመው ሰዎችን የሚያገሉ እና ሴቶች ላይ ጥቃት ለማድረስ አካውንታቸውን የሚጠቀሙ ሰዎችን አካውንት ማጥፋት ወይም ማመልከት የሚጠበቅብን ነገር ነው፡፡

ያስታውሱ፡ ይህንን ሁሉ ማድረግ ይቻላል!!!

የበይነ መረብ ደህንነት ምን ማለት እንደሆነ ጊዜ ሰጥተው ለማወቅ ይጣሩ እናም ሲጠቀሙ ማድረግ ያለብዎትን ጥንቃቄ ይተግብሩ፡፡ ለየት ያሉ ነገሮችን ማስተዋል እና ችግሮች ወደሌሎች ሳይሰራጩ መለየት መቻል ልዩ ችሎታ ስለሆነ እንደ አንድ ሀብት ይጠቀሙበት፡፡