የመረብ ደህንነት፣ ማጭበርበር፣ እና አይፈለጌ

ተሳታፊዎች የደህንነት ድክመቶች ተጠቅው እነሱን የሚመለከት መረጃ ለመሰብሰብ ስለሚሞክሩ አታላይ የመስመር ላይ ተጠቃሚዎች ይማራሉ። ተሳታፊዎች መስመር ላይ የመሆን ስጋት-አደጋዎች በተመለከተ ማብራራት ይችላሉ፣ ደህንነታቸው በተጠበቁ ቦታዎች ላይ የሚተገበሩ ስትራቴጂዎች ይነድፋሉ፣ አይፈለጌ መልእክቶችን ይለያሉ፣ እንዲሁም የይለፍቃላቸውን መጠየቅ ያለበት ማን እንደሆነ ያብራራሉ።

ማቴርያሎች

የአይፈለጌ የሚታደል ጽሑፍ

የመስመር ላይ ስጋተ-አደጋዎች

ክፍል አንድ

ለተማሪዎችዎ ይንገሩዋቸው

ኢንተርኔት በሚጠቀሙበት ጊዜ፣ ወደ ድረገጽ በመግባትዎ፣ የመስመር ላይ ተግባቦት በማድረግዎ፣ ወይንም ውሂብ በማውረድዎ ብቻ ራስዎስን ለስጋተ-አደጋ ሊያጋልጡ ይችላሉ። አንዳንድ ጊዜ እርስዎ የተጠቀሙባቸው ድረገጾች፣ በተመሳሳይ አውታረመረብ ላይ ያሉ ሰዎች፣ ወይንም ሶስተኛ ወገኖች የእርስዎን መገኛ ቦታ ወይንም ሌላ እርስዎን የሚመለከት መረጃ ሊያውቁ ይችላሉ።

ተማሪዎችዎን ይጠይቁ

የመስመር ላይ ደህንነት ተጋላጭነትን እንደ ክፍተት በመጠቀም የእርስዎን ማንነት የሚገልጽ መረጃ ሊያይ የሚችል አካል ማነው?

1. አታላይ ጠላፊዎች፣ የመንግስት የስለላ አካላት፣ ወዘተ መልሶች ሊሆኑ ይችላሉ።

ለተማሪዎችዎ ይንገሩዋቸው

ድረገጹን በሚያስሱበት ጊዜ፣ ልክ የኢንተርኔት አቅራቢዎች እንደሚያደርጉት ሁሉ ጠላፊዎችም የእርስዎን ውሂብ ሊሰበስቡ ይችላሉ። በእርስዎ እና እየተጠቀሙበት ባለው ድረገጽ(ጾች) መካከል ደህንነቱ የተጠበቀ ግንኙነት መኖር አለበት። ግንኙነትዎ ምንም ይሁን ምን፣ ብዙ ድረገጾች በብዙ ፕላትፎርሞች የእርስዎን የአጠቃቀም ሁኔታ ለመከታተል ይሞክራሉ። እርስዎ ማን እንደሆኑ ለማወቅ በሚያደርጉት ሙከራ የእርስዎን አሳሽ፣ መገኛ ቦታ፣ እንዲሁም ሌላ የአጠቃቀም ሁኔታ ሊያዩ ይችላሉ።

ተማሪዎችዎን ይጠይቁ

ለምንድነው አታላይ ጠላፊዎች የእርስዎን መረጃ መስመር ላይ ማግኘት የሚፈልጉት? ሰዎች ምን አይነት መረጃ ነው እየፈለጉ ያሉት? እርስዎ ከፍተው ያልገቡበት ድረገጽ ለምንድነው የእርስዎን ማንነት መከታተል የሚፈልገው?

1. ማንኛውም የምን እንደሆነ የሚታወቅ መረጃ እና ማንኛውም ሊሸጥ ወይንም ለገንዘባዊ ትርፍ ሊጠቅም የሚችል መረጃ።

ማልዌር ምን እንደሆነ የሚያውቅ ሰው አለ? ምን ሊያደርግ ይችላል?

ለተማሪዎችዎ ይንገሩዋቸው

ማልዌር እርስዎ ሳያውቁት በድብቅ ኮምፒዩተርዎ ላይ የሚንቀሳቀስ ጎጂ ኮድ ነው። አንዳንድ ማልዌር ከየትኛውም የኮምፒዩተርዎ ክፍል፣ ከሃርድ ድራይቭዎ እንዲሁም ከአሳሽ ውሂብዎ ውሂብ ሊሰበስብ ይችላል። በተጨማሪ ጠላፊዎች ኮምፒዩተርዎ ተቆጣጥሮው በፈለጉት መንገድ እንዲጠቀሙበት ይፈቅድላቸዋል። አብዛኞቹ ማልዌር ገንዘብ ለማግኘት አሳሽዎ ላይ እንደ የባንክ ወይን የተጨማሪዎችዎ ላይ ደህንነታቸው የተጠበቁ ፖርታሎች መስለው በመቅረብ በማስታወቂያነት የሚሰሩ ቀለል ያሉ ድረገጾች ያተቃልላሉ።

ተማሪዎችዎን ይጠይቁ

ራስዎን ከማልዌር፣ ስለላ፣ ወይንም ከክትትል ለመከላከል ምን ማድረግ ይችላሉ?

ለተማሪዎችዎ ይንገሩዋቸው

አገናኞች፣ ማስታወቂያዎች፣ ወይንም የማህበራዊ ሚድያ ልጥፎች ጠቅ በሚያደርጉበት ጊዜ ጠንቃቃ ይሁኑ። ያገኙት URL ከጠበቁት ጋር የሚዛመድ ነው? ራስዎ እንደገና ሲጽፉት ወይንም ድረገጽ ሲፈልጉ ወደ ተመሳሳይ ገጽ ይወስዶታል? ጥሩ ደንብ የሚባለው SSL / TLS ወደ ማንኛውም ወሳኝ መለያ የሚገረግ ከፍቶ መግቢያ ገጽ መከላከል አለበት የሚል ነው (ለምሳሌ፣ Google, Facebook, Twitter, ወይንም የባንክ ሒሳቦች)። SSL/TLS እርስዎ ትክክለኛ URL በሚጽፉበት ጊዜ ተመሳሳይ አውታረመረብ ላይ የሚገኝ ጠላፊ ወደ እርስዎ የውሸት ድረገጽ እንዳይልክልዎ ይከላከላል።

አንዳንድ ድረገጾች እነዚያ ፕላትፎርሞች የኮዲንግ ስህተት በሚፈጽሙበት ጊዜ ኮድ ተጠቅመው የእርስዎን የማንነት መረጃ ወይንም የመስመር ላይ መለያዎች ለማግኘት ይሞክራሉ። ከዚያ የእርስዎን መለያ ተጠቅመው ወደሌሎች አይፈለጌ መልእክት ሊልኩ ይችላሉ።

ሶፍትዌሮችን ከሚታመኑ ምንጮች ብቻ አውርደው ይጫኑ እንዲሁም ተፈጻሚዎችን (.exe, .pkg, .sh, .dll, or .dmg ተጨማሪዎች) መቼ ማውረድ እንዳለብዎም ልብ ይበሉ። ማስፈጸሚያዎች ማናቸውም ድርጊትን የሚፈጽሙ ነገሮች ናቸው። አንዳንድ ጊዜ፣ እነዚህ መጥፎ ድርጊቶችም ሊሆኑ ይችላሉ። ለምሳሌ፣ የሆነ ሰው የሌላ ሰው ሀርድ ድራይፍ ለመሰረዝ ማስፈጸሚያ ጽሑፍ ሊጽፍ ወይንም የውሸት አሳሽ ሊጭን ይችላል። ለዚህ ነው ከሚታመኑ ምንጮች ብቻ ይዘቶችን መጫን የሚኖርብዎ።

ከማልዌር እንቅስቃሴ የሚከላከልልዎ ጸረ-ቫይረስ መጠቀም ይችላሉ። አንዳንድ ጸረ-ቫይረስ ሶፍትዌሮች ከኮምፒዩተርዎ ጋር አብረው ይመጣሉ (ለምሳሌ፣ Microsoft Security Essentials for Windows); እንደ Apple ኮመፕዩተሮች የመሳሰሉ ከወና ስርአቶች ደግሞ ከማይታመኑ ምንጮች የተገኙ ሶፍትዌሮች እንዳይጫኑ የሚገታ የደህንነት ቅንብሮች አላቸው። እነዚህን ቅንብሮች ችላ ከማለትዎ በፊት በጥልቀት ያስቡ።

በተጨማሪም ድረገጾች እርስዎ ማን እንደሆኑ መለየት እንዲከብዳቸው ለማድረግ ተሰኪዎችን የሚያግዱ ተመስፋፊያዎችን ለማሰስ ሊተጉም ይችላሉ። ይሁን እንጂ ተመሳሳይ ተሰኪ እንደ ቪድዮ የማየት ችሎታ የመሳሰሉ የድረገጾቹ አቅሞችንም ሊገታ ይችላል። ማስፋፊያዎችን የመጫን እና ያለመጫን ውሳኔ የእርስዎ ምርጫ ነው እንዲሁም የእርስዎ ከመስመር ላይ ደህንነት አንጻር ጥቅሞችና ጉዳቶችን የማዛን ጉዳይላ ይወሰናል። እኔ ምን ያህል ለክትትል የማልመች ሆኜያለሁ የሚሉ ጥያቄዎችንም ከግምት ማስገባት አለቦት? የግላዊነቴ ዋጋ ምን ያህል ነው? ይህ ይዘት ምን ያህል ያስፈልገኛል (ለምሳሌ፣ የአሳሽ ማስፋፊያ ቪድዮ የሚያቀርብ ተሰኪ በሚገታበት ጊዜ)?

የደህንነት ማቀናበሪያዎች

ክፍል አንድ

የክላስ መስተጋብር

እባክዎ ልብ ይበሉ: የዚህ እንቅስቃሴ ይዘት በከፊል “እንቅስቃሴ #1 ላይ ተካቷል: የመስመር ላይ ስጋተ-አደጋዎች።” እንቅስቃሴ #1 ላይ ተሳትፈው ከሆነ ወይንም ከዘለሉት፣ ይህንን ማቴርያል እንደገና ሊሄዱበት ይፈልጉ አይፈልጉ ውሳኔዎን እንቀበላለን።

ተማሪዎችዎን ይጠይቁ

ኢንተርኔት በሚጠቀሙበት ጊዜ ደህንነትዎ የተጠበቀ መሆኑ እና አለመሆኑ ያውቃሉ?

ለተማሪዎችዎ ይንገሩዋቸው

ተገቢ ቅድመጥንቃዎች ሳያደርጉ፣ ራስዎን ከእነዚህ የመስመር ላይ ስጋተ-አደጋዎች በተሳካ ሁኔታ መጠበቅ ፈጽሞ አይቻልም እንኳ ባይባል ከባድ ነው [ያየከዚህ ቀደም ክፍል ላይ የተጠቀሱት።]

አዳዲስ የመስመር ላይ ስጋተ-አደጋዎችም በየጊዜው ይፈጠራሉ፣ ስለዚህ ንቁ ሆኖ መቆየት ጠቃሚ ነው።

ተማሪዎችዎን ይጠይቁ

አንድ የራሱ ድረገጽ በጣም ጠቃሚ መሆኑ ካሰመነዎት ምን ማድረግ ይኖርበታል?

እነዚህን ስጋተ-አደጋዎች የሚያስወግዱባቸው ወይንም የሚቀንሱባቸው ማቀነባበሪያዎች አሉ። የሚያውቅ ሰው አለ?

ለተማሪዎችዎ ይንገሩዋቸው

HTTPS በኢንተርኔት የሚያልፍ ውሂብ ለማመስጠር ድረገጾች የሚጠቀሙበት ስተንደርድ ነው። ምስጠራ የእርስዎ ግንኙነት ላይ የሚገኝ ውሂብ ሶስተኛ ወገን በቀላሉ እንዳያየው ሊከላከል ይችላል። ተጨማሪ ደህንነት ይሰጣል ስለዚህ “ https://” ከሚጠቀሙበት URL (ለምሳሌ፣ https://www.mysite.com) በፊት በማስገባት በማንኛውም አሳሽ ላይ መጠቀም ይቻላል። ይሁን እንጂ፣ ሁሉም ድረገጾች HTTPS ይደግፋሉ ማለት አይደለም።

1. የድር ጣብያ ላይ HTTPS:// በማስቀደም ሰንሲቲቭ መረጃ (ለምሳሌ፣ የይለፍቃላቶች፣ የክረዲት ካርድ መረጃ) ብቻ ነው ማስገባት ያለብዎ።

2. ሁልጊዜ HTTPS እየተጠቀሙ ስለመሆንዎ እርግጠኛ ለመሆን የሶፍትዌር ማቀነባበሪያዎችን መጠቀም ይችላሉ።
3. አብዛኞቹ ትልልቅ አሳሾች የ HTTPS ግንኙነቶችን የሚያመላክት የቁልፍ እናት የሚመስል የድህንነት አመልካች አላቸው።

4. ይሁን እንጂ፣ HTTPS የእርስዎን ሙሉ ደህንነት ሊያረጋግጡ አይችሉም ምክንያቱም አንዳንድ የአጭበርባሪዎች ድረገጾም HTTPS ይደግፋሉና። HTTPS የግንኙነቱን ደህንነት ይጠብቃል ግን ድረገጹ ጥሩ ተዋናይ መሆኑን ማረጋገጥ አይችልም።

ደህንነታቸው የተጠበቁ ሶኬቶች ሽፋን (SSL)/የትራንስፖርት ሽፋን ደህንነት (TLS) ደህንነቱ የተጠበቀ HTTPS እንዲኖር የሚያደርግ ቴክኖሎጂ የሚጠራባቸው ስሞች ናቸው። SSL/TLS እውነተኛ ቁልፍ የሚመስሉ ዲጂታል የምስጠራ ቁልፎች ይጠቀማል። ለጓደኛዎ በብጣሽ ወረቀት ሚስጢር ቢጽፉለት፣ ወረቀቱን ያገኘ ሰው ሚስጢሩን ማየት ይችላል። እንደሱ ከማድረግ ይልቅ፣ እርስዎ የቁልፍ ቅጂ በአካል ሰጡዋቸው፣ ከዛ ሚስጢሮችዎ በተቆለፉ ተመሳሳይ ቁልፎች ተላኩ ብለን እናስብ። የሆነ ሰው ሳጥኑን ቢያገኘው እንኳ፣ ቁልፉን ሳያገኝ ሚስጢርዎን ማየት አይችልም። የሆነ ሰው ሳጥኑን በተመሳሳይ ሳጥን ሊተካው ቢሞክር፣ እርስዎ ቁልፍዎ ሊሰራ እንደማይችል ልብ ይላሉ። SSL/TLS በተመሳሳይ መንገድ ይሰራል፣ ግን ከድረገጽ ጋር ነው።

የአሳሽ ደህንነት አመልካቾች ተስፋፊ የቅቡልነት (EV) ሰርትፊኬት መረጃም ይናገራሉ። EV ሰርቲፊኬቶች ማንነታቸው ለሰርትፊኬት ባስልጣን ለሰጡ ድረገጾች የሚሰጡ ሰርትፊኬቶች ናቸው። አሳሾች ላይ፣ አንዳንድ ጊዜ EV አመልካቹ የድሩ ስም ወይንም ከአድራሻ ጽላቱ ቀጥሎ ያለው መመዝገቢያ ተቋም ቅርጽ ይይዛል። EV ሰርቲፊኬቶች ማንነታቸው ለሰርትፊኬት ባስልጣን ለሰጡ ድረገጾች የሚሰጡ ሰርትፊኬቶች ናቸው። አሳሾች ላይ፣ አንዳንድ ጊዜ EV አመልካቹ የድረገጹ ስም ወይንም ከአድራሻ ጽላቱ ቀጥሎ ያለው መመዝገቢያ ተቋም ቅርጽ ይይዛል። የሆነ ድረገጽ ላይ ያዩት ይዘትን የሚጠረጥሩ ከሆነ፣ “ሰርትፊኬት ተመልከት” የሚለው ላይ ጠቅ በማድረግ ሰርትፊኬቱ ላይ ያለው URL አሳሹ ላይ ካለው URL ጋር አንድ አይነት መሆናቸውን ማየት ይችላሉ። [ተሳታፊዎች “ሰርትፊኬት ተመልከት” የሚለውን እንዴት ማግኘት እንደሚቻል ለተሳታፊዎቹ በፕሮጀክሽን ስክሪን ማሳየት ጠቃሚ ሊሆን ይችላል። ወደዚህ የሚናኙበት መንገድ እንደየ አሳሹ ይለያያል። ለምሳሌ፣ Chrome ላይ “ተመልከት” ከሚለው ስር “ሰሪ” ላይ ጠቅ ታደርግ እና ከዛ “የሰሪ ማቀናበሪያዎች” ላይ ጠቅ ታደርጋለህ ከ “የሰሪ ማቀናበሪያዎች” ላይ “ደህንነት” ትር ላይ፣ ከዛ ደግሞ “ሰርትፊኬት ተመልከት” ላይ ጠቅ ያደርጋሉ።

ከማይታመኑ ምንጮች የተገኘ ሶፍትዌር አለመጠቀም እንዳለ ሆኖ፣ ጸረ- ቫይረስ ሶፍትዌርም እርስዎን የማይታመኑ ገጾች ከመጎብኘት እና ማልዌር ከማውረድ ሊከላከልልዎ ይችላል።

“ማጭበርበር” በዋናነት ሕጋዊ አካል መስሎ በሚቀርብ አካል በኢሜይል የሚከናወን ተግባር ነው። ከዛ የይለፍቃልዎ ይጠይቃሉ፣ ይህ የሚያደርጉት በኢሜይል እንዲልኩልዎ ወይንም በደ የውሸት ድረገጽ እንዲያስገቡልዎ ተስፋ በማድረግ ነው። የአይፈለጌ ማጣሪያዎች አንዳንድ እንደዚህ አይነት ኢሜይሎች የገቢ መልእክት ሳጥንዎ ላይ እንዳይታዩ ሊከለክሉ ይችላሉ። የአይፈለጌ ማጣሪያዎች ለማሻሻል፣ የገቢ መልእክት ሳጥንዎ ላይ ያገኙት ማንኛውም የሚጠራጠሩት ኢሜይል የአይፈለጌ ምልክት ያድርጉለት።

ተማሪዎችዎን ይጠይቁ

ኮምፒዩተርዎን ሊጎዱ የሚችሉ ፋይሎች ድንገት ከማውረድ ራስዎን ለመከላከል ምን እርምጃዎች መውሰድ ይኖርብዎታል?

ለተማሪዎችዎ ይንገሩዋቸው

ሁልጊዜ ከታማኝ ድረገጾች እያወረዱ መሆንዎ ደጋግመው ያረጋግጡ። የማያውቁዋቸው የኢሜይል አባሪዎች ስለመክፈት እንዲሁም ድንገቴ ድረገጾች እና የስህተት መልእክቶች ላይ ጠቅ ስለማድረግ እጅግ ጠንቃቃ ይሁኑ። በተጨማሪ እርስዎ ዝነኛ ጸረ-ማልዌር ፕሮግራሞችን ኮምፒዩተርዎ ላይ መጫንም እንደ አማራጭ ሊወስዱ ይችላሉ።

የይለፍቃል ማጋራት

ክፍል አንድ

ተማሪዎችዎን ይጠይቁ

የይለፍቃልዎ ማጋራት ጥሩ የሚሆነው መቼ ነው ብለው ያስባሉ?

1. የጋራ መለያዎች (ለምሳሌ Netflix) መልስ ሊሆኑ ከሚችሉት ውስጥ አንዱ ነው።

የይለፍቃልዎ ካማጋራትዎ ጋር ተያይዘው ሊመጡ የሚችሉ ስጋተ-አደጋዎች ይግለጹ?

1. አታላይ ሰው የይለፍቃልዎን ካገኘ፣ መለያዎ ሊጠለፍ ይችላል። የይለፍቃል ማጋራት የሆነ ሰው ወደ መለያዎ መግባት እንዲችል እንደመፍቀድ ማለት ነው። ተመሳሳይ የይለፍቃል ሌሎች ድረገጾች ላይም ጥቅም ላይ የሚውል ከሆነ፣ ወደ እነዚያንም መግባት ይችላሉ ማለት ነው።

ለተማሪዎችዎ ይንገሩዋቸው

የይለፍቃልዎ እከፍተው ለሚገቡበት መተግበሪያ ካልዎነ በስተቀር በፍጹም ለሌላ አለማጋራት የተለመደ አሰራር ነው። ቀደም ሲል እንደተገለጸው፣ ማጭበርበር የሰዎች የይለፍቃል ለማግኘት የሚደረግ የመሸወድ ተግባር ነው።

ይሁን እንጂ፣ አንዳንድ ሰዎች መለያዎ አደጋ ውስጥ እንደሆነ በመግለጽ የእርስዎን መለያ ከፍተው ለመግባት የይለፍቃልዎ እንዲሰጡዋቸው በግልጽ ሊጠይቅዎ ይችላሉ። ከነዚህ ሰዎች ውስጥ አንዳንዶቹ በቅንነት የሚጠይቁ ሊሆኑ ይችላሉ፣ ለምሳሌ የሆነ መለያዎ ላይ እርስዎን ግራ እያጋባ ያለ ነገር በማሰስ ረገድ ሊረዳዎት የሚፈልግ ጓደኛዎ። ነገርግን በተለይ ያንን የይለፍቃል ለብዙ መለያዎች የሚጠቀሙበት ሲሆን ለሰዎች ማጋራት እንዝህላልነት ነው። የይለፍቃልዎ ለማጋራት ካቀዱ፣ ሌላ ቦታ ላይ ጥቅም ላይ እንደማይውል ያረጋግጡ እንዲሁም የይለፍቃል አስተዳዳሪ ተጠቅመው ያጋሩ።

አንዳንድ ጊዜ፣ የእርስዎን ይለፍቃል የሚጠይቁ ሰዎች እንደ ወላጆችዎ፣ አስተማሪዎችዎ፣ ወይንም አሰሪዎ የመሳሰሉ እርስዎ የሚያምኑዋቸው ሰዎች ሊሆኑ ይችላሉ። ምንም እነዚህ አዋቂዎች ቢያምኑዋቸውም፣ ለምን ይህንን ጥያቄ እንዳቀረቡ እና የይለፍቃሎችዎ እንዴት እንደሚይዙዋቸው በሚመለከት ውይይት ማድረግ ለሁላቹም (ለእርስዎ እና ለእነሱ) አወንታዊ ተግባር ነው። በተለይ አዋቂዎቹ የቤተሰብዎ አባላት ካልሆኑ፣ እርስዎ የይለፍቃልዎ ለእነሱ እንዲሰጡ የሚያስገድድ ሕግ ወይንም ደንብ አለ ብለው የሚያምኑ እንደሆነ ይጠይቁዋቸው።

እንደ የሕግ አስፈፃሚ ሀላፊ የመሰሰሉ እርስዎ በግል የማያውቁዋቸው የቤተብዎ አባል ያልሆኑ አዋቂዎች የይለፍቃልዎ እንዲሰጡዋቸው ሲጠይቁዎ፣ ሕጎችን እና ደንቦችን የተመለከቱ ጥያቄዎችን በትህትና እና በግልጽ መጠየቅ እጅግ ተቃሚ ነው። የፖሊስ ሀላፊ ወይንም ሌላ የመንግስት ባለስልጣን የማህበራዊ ሚድያ የይለፍቃልዎ ሲጠይቅዎ፣ ተረጋግተው በክብር ይመልሱላቸው። ለምን እንደሚጠይቁዎ ይጠይቁዋቸው እንዲሁም ይህንን መረጃ ከእርስዎ እንዲያገኙ የትኛው ሕግ(ጎች) ወይንም ደንብ(ቦች) መብት እንደሰጡዋቸው ይጠይቁዋቸው።

ወላጅዎ / ተንከባካቢዎ፣ አስተማሪዎ፣ የሕግ አስፈጻሚ ሀላፊ፣ የመንግስት ባለስልጣን፣ ወይንም ሌላ አዋቂ ጥያቄውን ያቀረቡበት ሁኔታ ከግምት በማስገባት፣ የይለፍቃሎችዎን ሊሰጡዋቸው ይችላሉ። ለምሳሌ እርስዎ የይለፍቃልዎ እንዲሰጡ በሕግ የሚገደዱ ሲሆን ወይንም እርስዎ የይለፍቃልዎ በማጋራትዎ ከሚከተለው ስጋተ-አደጋ ይልቅ የሚያገኙት ጥቅም ይበልጣል ብለው ሲያስቡ የይለፍቃልዎ ሊያጋሩ ይችላሉ።

አንድ አዋቂ የይለፍቃልዎ እንዲሰጡት ቢጠይቅዎ፣ እና ያንን ጥያቄ ለእርስዎ ምቾት ከፈጠረልዎ፣ ለጥያቄው ምላሽ ከመስጠትዎ በፊት ወላጅ / ተንከባካቢ ወይንም ታማኝ አዋቂ ያማክሩ።

ተማሪዎችዎን ይጠይቁ

የይለፍቃልዎ መስመር ላይ ማጋራት የሚችሉት በምን ሁኔታ ላይ ነው?

1. እርስዎ ድረገጹ ላይ ወደ የይለፍቃልዎ በሚመሩበት ጊዜ ብቻ ከፍተው ለመግባት ይሞክራሉ። ባልተመሰጠረ እና ደህንነቱ ባልተጠበቀ ኢሜይል ጨምሮ የይለፍቃልዎን ሌላቦታ ፈጽመው አያጋሩ።

ምድብ ሥራ

የሚታደል ጽሁፍ

ምድብ ስራ

ተሳታፊዎች በ 2-3 ቡድኖች ይከፋፍሉዋቸው። ለተሳታፊዎች የአይፈለጌ የሚታደል ጽሑፍ ያሰራጩ ከዛ በኋላ ተሳታፊዎች አይፈለጌን እንዴት መለየት እንደሚችሉ እንዱሁም የሆነ መረጃ ለሆኑ ግለሰቦች/ቡድኖች ማጋራት ይኖርባቸው እንደሆነ ለሌሎች ለማሳየት የሚጠቅም ፍሎውቻርት እንዲያዘጋጁ ያድርጉዋቸው።

ለተማሪዎችዎ ይንገሩዋቸው

እያንዳንዱን ኩነተ-ፍጻሜ ያንብቡ እና እያንዳንዱ መልእክት አይፈለጌ ስለመሆኑ እና አለመሆኑ እንዲሁም በኩነተ-ፍጻሜው ለሚገኙ ሰዎች መረጃ መጋራት ይኑርብዎ አይኑርብዎ ይወያዩ።

የክላስ መስተጋብር

ተሳታፊዎች ይህንን እንዲሰሩ 10 ደቂቃ ይስጧቸው። ከዚያ በኋላ፣ ቡድኖቹ ምላሾቻቸውን እንዲያጋሩ ይጠይቁዋቸው።

ተማሪዎችዎን ይጠይቁ

ይለፍቃልዎ በኢሜይል ማጋራት የሚኖርብዎ መቼ ነው?

ለተማሪዎችዎ ይንገሩዋቸው

ድረገጾች እና ኩባንያዎች ፈጽመው እርስዎ በኢሜይል የይለፍቃል እንዲልኩ አይጠይቁዎትም። ምንጩ ሕጋዊ ቢመስሎት ጭምር፣ ፈጽመው ይለፍቃልዎን በዚህ መንገድ ለማንም ማጋራት የለብዎትም። ኢሜይል ፈጽሞ አስተማማኝ ደህንነት ኖሮት አያውቅም።

ክፍል ሁለት

ምድብ ስራ

የሚቀጥለው መልመጃ በግል የሚሰራ ስለሆነ ተሳታፊዎች ከቡድኖቻቸው እንዲበተኑ ያድርጉዋቸው።

ተሳታፊዎች የየራሳቸው ፍሎውቻርት እንዲያዘጋጁ 15 ደቂቃ ይስጡዋቸው።

ለተማሪዎችዎ ይንገሩዋቸው

አሁን፣ በንጥል ወረቀት ላይ፣ ግለሰቡቹ እንዴት አይፈለጌ መልእክትን እንደሚለዩ እና እንዴት መረጃ መስመር ላይ ለሌሎች እንደሚያጋሩ ለማየት የሚያስችል ፍሎውቻርት ያዘጋጁ። ፍለውቻርትዎ የሚመሰረትበት አንድ ኩነተ-ፍጻሜ መጠቀም ጥሩ ሊሆን ይችላል; በሚታደለው ጽሑፍ ከቀረቡት ኩነተ-ፍጻሜዎች አንዱ ማለት ነው (እንደሱ ማድረግ ከመረጡ፣ እባክዎ የኩነተ-ፍጻሜው ቁጥር ከፍለውቻርቱ በላይ ይጻፉት)፣ ወይንም ሌላ አዲስ! የራስዎ ኩነተ-ፍጻሜ ንድፍ ለማዘጋጀት ከመረጡ፣ እባክዎ ከፍለውቻርትዎ በላይ በአጭር አንቀጽ ይግለጹት።

ተሳታፊዎች የየራሳቸው ፍሎውቻርት እንዲያዘጋጁ 15 ደቂቃ ይስጡዋቸው።