BritishRedCross

Home Office

የስደተኛ ሴቶች ዲጂታል የማኅልበት እና የግንኙነት ፕሮጀክት

ወርክሾፕን 3ን ለማጀብ መመሪያ

ዲጂታል

ይህ መመሪያ በዲጂታል የስደተኛ ሴቶች የማጎልበት እና ግንኙነት ፕሮጀክት አውደ ጥናቶችን ውስጥ ለሚሳተፉ ሴቶች እንደ ድጋፍ መሳሪያ ተዘጋጅቷል፡፡ ዒላማ ያደረገው የስደተኛነት ሁኔታ ያላቸው ፣ የሰብአዊ ጥበቃ ወይም የስደተኛ ቤተሰብ ውህደት ባላቸው እና UK በሚኖሩ ሴቶች ላይ ነው፡፡ ፕሮጀክቱ በሀገር ውስጥ ጉዳይ ቢሮ የስደተኛ ድጋፍ እና ውህደት ፈንድ የተደገፈ ነው፡፡

እነዚህ የቆዩ ሰነዶች እንዲዘጋጁ ድጋፍ ያደረጉትን የ VOICEs ኔትወርክ አባላት እና Voices Ambassadors ማመስገን እንፈልጋለን፡፡ ጽሁፎች በእንግሊዝኛ ፣ በአማርኛ ፣ በአረብኛ ፣ በፋርሲ ፣ በኩርዶች (ሶራኒ) በሶማሌ ፣ በትግርኛ እና በኡርዱ ይገኛሉ፡፡ በዚህ ወርክሾፖች ላይ መሳተፍ ያልቻሉ ስደተኛ ሴቶች አሁንም መረጃውን በእራሳቸው ፍጥነት ለማየት እና ለማሰስ አሁንም ጠቃሚ ሆኖ እንደሚያገኙት ተስፋ ይደረጋል፡፡

ይዘቶች

መቅድም 2

ቁልፍ ቃላት 3

ዲጂታል ደህንነት ምንድን ነው? 3

አስፈላጊ የዲጂታል ደህንነት ምክሮች 4

ጠንካራ የይለፍ ቃላት መኖር 4

የይለፍ ቃል አስተዳዳሪ ይጠቀሙ 4

ባለ ሁለት አካል ማረጋገጫ ያዘጋጁ 4

መሳሪያዎችዎን ከቫይረሶች መጠበቅ 4

የውሂብዎን ምትኬ ያስቀምጡ 5

ማጠቃለያ 5

በአገልግሎቱ ካልረኩ ምን ማድረግ እንደሚቻል 6

የተለመዱ ዓይነቶች ኦንላይን ስጋት 6

ተንኮል እና ማጭበርበሮች 6

ፊሺንግ 6

ደህንነታቸው የተጠበቀ እና ደህንነታቸው ያልተጠበቀ ድረ-ገጾች 8

በማጭበርበር ከተጠቁ ምን ማድረግ ይኖርብዎታል 9

ኦንላይን ግንኙነቶች 9

የፍቅር ስሜት ማጭበርበር 10

የሳይበር ጉልበተኝነት 10

ማባበል 10

ሴክስቲንግ እና የበቀል የወሲብ ስራ 11

የሳይበር ክትትል እና ቁጥጥር 11

የቤት ውስጥ ጥቃት ፣ ትንኮሳ እና ክትትል 12

ማጠቃለያ 13

መቅድም

ይህ መሳሪያ ለኢንተርኔት ተጠቃሚዎች የሚገኙትን ሁሉንም ስጋቶች እና የጥንቃቄ እርምጃዎችን ሙሉ በሙሉ መመርመር እና ማብራራት አልቻለም ነገር ግን አንዳንድ ቁልፍ ነጥቦች እና ተጨማሪ መረጃዎችን የት እንደሚያገኙ እንደሚያሳይ ተስፋ ያደርጋል፡፡

በዲጂታል ደህንነት ላይ ስንወያይ በጾታ ላይ የተመሠረተ ጥቃት ፣ በደል እና የወንጀል ጥሰቶች ዙሪያ ስሜታዊ እና ብዙውን ጊዜ አስጸያፊ በሆኑ ጉዳዮችን እንደምንነካ እናሳውቃለን፡፡ የእኛ ሰብአዊ ተልእኮ እና ምንም ጉዳት የማያስከትሉ መርሆዎች ሰዎችን በጾታ ላይ የተመሠረተ ጥቃትን ለመቋቋም በችሎታችን ውስጥ ያለውን እርምጃ እንድንወስድ የተጠራን ሲሆን ሰዎችን የሚያበረታቱ ምርጫዎችን እና እነሱን የሚጠብቁ ውሳኔዎችን እንዲያደርጉ ለመደገፍ መረጃን መስጠት ነው፡፡

በዚህ መመሪያ ውስጥ በሙሉ በጽሁፉ ውስጥ የተካተቱ አገናኞችን ያገኛሉ ፣ እነዚህን ቢጫኑ ወደተጠቀሰው ድረ-ገጽ ይወስደዎታል፡፡ ለምሳሌ ፣ እዚህ ቢጫኑ ወደ ብሪቲሽ ቀይ መስቀል ድረ-ገጽ ይወሰዳሉ። በሚቻልበት ጊዜ ወደ የተተረጎሙ ሀብቶች አገናኞችን ለማካተት ሞክረናል ፣ ግን በዚህ መመሪያ ውስጥ ያሉት ብዙ አገናኞች በእንግሊዝኛ ለሚገኙ መረጃዎች ናቸው፡፡ የራስ-ሰር የትርጓሜ ውስንነቶች የምንቀበል ቢሆንም ፣ በመመሪያ ሁለት ውስጥ ይህንን ተግባር እንዴት እንደሚጠቀሙበት መረጃ ሰጥተናል፡፡
ስለ ዲጂታል ደህንነት፣ አጠቃላይ መሳሪያዎችዎን እንዴት መከላከል እንደሚችሉ እና ራስዎን እና ሌሎችን ከኦንላይን አደጋዎች መጠበቅን ጨምሮ የሚረዱ እርምጃዎችን ከ www.getsafeonline.org.uk እና ከብሔራዊ ሳይበር ደህንነት ማዕከል www.ncsc.gov.uk ይገኛል። ኦንላይን ጥቃት ሰለባዎች ተጨማሪ መረጃ እና ድጋፍ ከ Stop Online Abuse – www.stoponlineabuse.org.uk ይገኛሉ። ለተጨማሪ መረጃ ወይም ድጋፍ ማንኛውንም የሥርዓተ-ፆታ ላይ የተመሠረተ ጥቃት ፣ የቤት ውስጥ በደል ወይም ትንኮሳ ለመቋቋም ወይም ሪፖርት ለማድረግ ከስደተኛ ወይም ከብሔራዊ የቤት ውስጥ ጥቃት የእገዛ መስመር ጋር ይገናኙ www.refuge.org.uk / www.nationaldahelpline.org.uk 0808 2000 247።

ወዲያውኑ የሚያሳስብዎት ነገር ካለ ወይም ወንጀል ለማስመዝገብ ከፈለጉ ፖሊስን ያነጋግሩ - 999 (ድንገተኛ) - 101 (ድንገተኛ ያልሆነ)

ቁልፍ ቃላት

ዲጂታል ደህንነት - ኢንተርኔት ሲጠቀሙ ራስዎን ፣ ሌሎችን እና የግል መረጃዎን ደህንነት ለመጠበቅ የሚረዱ ተግባሮች እና ልምዶች
ከሌሎች ጋር መስተጋብር - በሰዎች መካከል ካለው መስተጋብር ጋር የሚዛመድ
ኦንላይን ስጋት - በኢንተርኔት አማካኝነት የማይፈለግ ክስተት ወይም እርምጃን የሚያስከትል አደጋ ወይም ችግር
የይለፍ ቃል - ወደ ኮምፒተር ስርዓት ወይም አገልግሎት የሚያስገባ ምስጢራዊ ተከታታይ ፊደል/ቁጥር
ደህንነቱ የተጠበቀ - ደህንነቱ የተጠበቀ እና ስጋት የሌለበት ፣ ለአደጋ ወይም ለጉዳት ያልተጋለጠ፡፡

ዲጂታል ደህንነት ምንድን ነው?

ዲጂታል ደህንነት ማለት እራስዎን (እና መረጃዎን) ኦንላይን ከሚደርሱ አደጋዎች እንዴት መጠበቅ እንደሚችሉ መገንዘብ እና ማወቅ ማለት ነው፡፡ ብዙውን ጊዜ ዲጂታል ደህንነት ማለት ለሳይበር-ወንጀል ፣ ለማጭበርበር ወይም ለዛቻ ተጋላጭነት እንዳይጋለጡ የሚያደርጉዎ ጥቂት ጥሩ ልምዶች ማለት ነው፡፡ ይህ ወንጀለኞች መረጃን ወይም ገንዘብን ከእነሱ ጋር እንዲካፈሉ ወይም የግል ሕይወትዎን ለመውረር የሚጠቀሙባቸውን አንዳንድ ብልሃቶችን ማወቅን ያጠቃልላል፡፡

ኦንላይን በጣም የተለመዱት የስጋት ዓይነቶች የሚመጡት ከሚከተለው ነው፡

- የግል መረጃዎን ወይም የመለያ ዝርዝሮችዎን ለመስረቅ (“ለመጥለፍ”) የሚሞክሩ ቫይረሶች እና ተንኮል-አዘል ዌር ወይም እርስዎን ሊሰልሉዎ የሚችሉ ፕሮግራሞችን ለመጫን
- ወንጀለኞች መረጃን አሳልፈው እንዲሰጡ ሊያሳምኑዎት የሚሞክሩበት ኦንላይን ማጭበርበር
- ኦንላይን ማንነታቸው አለመታወቁን ተጠቅመው እርስዎን ለማዋከብ ፣ ለማንሳቆል ወይም ለመቆጣጠር የሚጠቀሙ ጉልበተኞች ፣ ተለጣፊዎች እና ተሳዳቢዎች፡፡

ኦንላይን ማስፈራሪያዎች በገንዘብ ፣ በስሜታዊ እና በግል ደህንነት ላይ ተጽዕኖ የማድረግ አቅም አላቸው። አእምሮ ውስጥ ይህን ሚዛናዊነት ፣ በአስፈላጊ ሁኔታ በመገንዘብ ፣ ስለ ዲጂታል ደህንነት ግንዛቤ ሰዎች ኦንላይን ያላቸውን እምነት እንዲያሳድጉ ያግዛቸዋል።

አስፈላጊ የዲጂታል ደህንነት ምክሮች

ጠንካራ የይለፍ ቃላት መኖር

ኢሜል እና ሌሎች ሁሉም መለያዎች ሌሎች በመለያዎ ላይ እንዳይደርሱ ለመከላከል በይለፍ ቃል ፣ በቁልፍ ተቆልፈዋል፡፡ የይለፍ ቃሉን ውስብስብ ወይም “ጠንካራ” ማድረግ አንድ ሰው ወደ የግል መረጃዎ እንዳይገባ ለመከላከል የተሻለው መንገድ ነው፡፡

ጠንካራ የኢሜል ይለፍ ቃል መኖሩ አስፈላጊ ነው፡፡ ጠላፊ ወደ ኢሜልዎ ከገባ 'የይለፍ ቃል መርሳት' ባህሪን በመጠቀም ሁሉንም ሌሎች የመለያ ይለፍ ቃላትን እንደገና ማስጀመር እና በሁሉም መለያዎችዎ ላይ ጥንቃቄ የሚፈልጉ የግል መረጃዎችን ማግኘት ይችላሉ፡፡

ጠላፊዎች ብዙዎቻችን እንደ 123456 ፣ በሕይወታችን ውስጥ አስፈላጊ ቀን ወይም የልጅ ስም ያሉ የይለፍ ቃሎችን እንደምንመርጥ ያውቃሉ - በቀላሉ ሊገመት የሚችል ማንኛውንም ነገር ለመጠቀም አይሞክሩ፡፡ ቀላል የይለፍ ቃላት በፍጥነት ሊገመቱ ይችላሉ ፣ ግን ጥሩ የይለፍ ቃል በወንጀለኞች ለመገኘት አስቸጋሪ ናቸው። አንድ ለመፍጠር ጊዜ መስጠቱ ተገቢ ነው፡፡

አዲስ ጠንካራ የይለፍ ቃል ለመፍጠር እነዚህን ደረጃዎች ይከተሉ፡

1. ሶስት የዘፈቀደ ቃላትን ይቀላቀሉ፡ ለምሳሌ ፣ ምንጣፍ (rug)፣ እሳት (fire)፣ ሹካ (fork) በመቀጠል ምንጣፍእሳትሹካ (rugfirefork) ይበሉ፡፡
2. አቢይ ሆሄን ያክሉ ፣ ለምሳሌ ፣ RugFireForK
3. ቁጥሮች አክል ፣ ለምሳሌ ፣ 19RugFireForK90 ፣ እና
4. የይለፍ ቃሉን የበለጠ ውስብስብለማድረግምልክቶችንያክሉ! 19RugFireForK90!

ጠላፊዎች በሚሊዮኖች የሚቆጠሩ የማይሰሩ የይለፍ ቃሎች አሏቸው እና ሦስት የዘፈቀደ ቃላቶችን ዝርዝር ለእርስዎ ልዩ ሊሆኑ እና ሊገመቱ የማይችሉ አዳዲስ የይለፍ ቃሎችን ለመፍጠር ቀላሉ መንገድ፡፡ በየጊዜው የይለፍ ቃላትዎን እንዲለወጡ እና ለሁሉም መለያዎችዎ አንድ ዓይነት የይለፍ ቃል እንዳይጠቀሙ በጥብቅ ይመከራል፡፡ አዳዲስ የይለፍ ቃላትን ለመፍጠር የሚቸገሩ ከሆነ የይለፍ ቃል ማመንጫ እንዲሁ ጥሩ ምርጫ ነው።

የይለፍ ቃል አስተዳዳሪ ይጠቀሙ

'ጠንካራ' የይለፍ ቃሎችን አላስታውስም ብለው ከተጨነቁ፣ የይለፍ ቃል አስተዳዳሪ መጠቀም ይችላሉ፡፡ የይለፍ ቃል አስተዳዳሪዎች አሳሹ ለእርስዎ የይለፍ ቃል እንዲያስታውስ የይለፍ ቃልዎን በድር አሳሽ (ለምሳሌ እንደ Google Chrome ወይም Microsoft Edge) ማስቀመጥ ማለት ነው፡፡ መጥፎ ወይም ደካማ የይለፍ ቃሎችን ከመጠቀም የበለጠ ደህንነታቸው የተጠበቀ ነው ነገር ግን መሳሪያዎን ቢያጡ እነሱን ለመጠበቅ እነሱን ያስታውሱ፡፡ በፀረ-ቫይረስ እና ኦንላይን ደህንነት ላይ የተሰማሩ አንዳንድ ኩባንያዎች የፀረ-ቫይረስ መሣሪያዎቻቸውን ከገዙ የይለፍ ቃል አስተዳዳሪን እንደ መስፈርት ያቀርባሉ ፣ ሌሎች ኩባንያዎች በራሳቸው የይለፍ ቃል አስተዳዳሪዎችን ያቀርባሉ፡፡

ባለ ሁለት አካል ማረጋገጫ ያዘጋጁ

ባለ ሁለት አካል ማረጋገጫ ከእርስዎ የይለፍ ቃል በተጨማሪ ሌላ መረጃ በመጠየቅ በመለያዎ ላይ ሌላ የጥበቃ ደረጃ ያክላል፡፡ ይህ የይለፍ ቃልዎ ቢኖራቸውም ሌሎች ወደ መለያዎችዎ እንዳይገቡ ለማቆም ይረዳል። ለታዋቂ ኢሜል እና ለማህበራዊ አውታረመረቦች ሁለት መረጃን ማረጋገጥ እንዴት ማድረግ እንደሚቻል መመሪያ **በብሔራዊ ሳይበር ደህንነት ማዕከል(National Cyber Security Centre)**ድረ-ገጽላይእዚህ ይገኛል።

መሳሪያዎችዎን ከቫይረሶች መጠበቅ

ቫይረሶች በድረ-ገጾች ፣ በኢሜል አገናኞች ፣ በአባሪዎች ወይም በተንቀሳቃሽ ሚዲያ (እንደ የ USB ስቲኮች) የሚተላለፉ የተደበቁ ፕሮግራሞች ናቸው፡፡ እነሱ ብዙ ብጥብጥን ሊያስከትሉ እና ከኮምፒዩተርዎ ወይም ከሂሳብዎ ሊያግዱዎ ፣ የግል መረጃዎን ለመሸጥ ወይም ለመጠቀም መስረቅ ፣ ገንዘብዎን ለመውሰድ ወይም በቤትዎ ውስጥ እንኳን ሊመለከቱዎት ይችላሉ፡፡ በሚያሰጋ ሁኔታ ፣

ሁሉም ሰው መሣሪያዎቻቸውን ከእነዚህ አደጋዎች እንዴት እንደሚጠብቁ ወይም እርምጃዎችን እንደሚወስዱ አያውቁም። ONS እንደዘገበው በ 2020 ስማርት ስልክ ካላቸው ጎልማሶች ውስጥ 17% የሚሆኑት በስማርት ስልካቸው ላይ ደህንነት ያልነበራቸው ሲሆን 32% የሚሆኑት ደግሞ ደህንነት ስለመኖራቸው ወይም እንደሌላቸው አያውቁም፡፡

እንደ አንድ የጥበቃ ሠራተኛ ሁሉ **ጸረ-ቫይረስ** በላፕቶፕ ፣ በታብሌት ወይም በስልክ ላይ የተጫነ እነዚህ ችግር ፈጣሪዎች ፕሮግራሞችን በመሣሪያዎችዎ ላይ እንዳይበከሉ የሚያቆም መሣሪያ ነው፡፡ እንደ ኮምፒተር ፣ ላፕቶፕ ፣ ታብሌት ወይም ስማርት ስልክ ያሉ የጸረ-ቫይረስ መከላከያ የሚከተሉትን የመሰሉ የተለመዱ ስጋቶችን ለመከላከል በጣም አስፈላጊ ነው፡

- **ትጃንስ (Trojans)፣** ማውረድየሚፈልጉትንፕሮግራም የሚመስል (እንደ ጸረ-ቫይረስ ፕሮግራም ፣ ፎቶ ወይም ነፃ ፊልም ያሉ) ግን በኮምፒተር ወይም በስልክ ሲጭኑ ንቁ ሆኖ የሚሰራ ተንኮል አዘል ሶፍትዌር (ዌር) አላቸው፡፡
- **ስፓይዌር (Spyware)፣** መረጃን የሚከታተል እና ለወንጀል ዓላማ በፒሲዎ ላይ የሚያደርጉትን የሚመለከት ፣
- **አድዌር (Adware)** ነገሮችን ለመሸጥ የሚሞክሩ ብቅ-ባይ መስኮቶችን የሚከፍት፡፡
- **ራንሰምዌር (Ransomware)** ከመሣሪያዎ ውጪ እርስዎን የሚቆልፍ እና ክፍያ የሚጠይቅ።
- **ስፓም (Spam)፣** በክፍት ድር ግንኙነቶች በኩል ወደ ስርዓትዎ የሚገቡ ዎርምስ የሚባሉ አይፈለጌ መልእክት “ስፓም” ኢሜሎችን ወደ እውቂያዎችዎ ለመላክ የሚያባዛ ፕሮግራሞችን የሚያመነጩ፡፡ የማይፈለግ የኢሜል ግንኙነት እንደ **አይፈለጌ መልእክት (ስፓም)** ወይም **አላስፈላጊ ኢሜል (ጀንክ)** ተብሎ ይጠራል ፡፡ አይፈለጌ መልእክት ኢሜል በቀላሉ ሊረብሽ ይችላል ፣ ግን ሰዎችን ለማጭበርበር እና የተሳሳተ መረጃን ለማሰራጨትም ሊያገለግል ይችላል።

አብዛኛዎቹ ስርዓቶች ቀድሞውኑ የተጫኑ አንዳንድ **ጸረ-ቫይረስ ወይም የስፓይዌር** ጥበቃ ይኖራቸዋል ፣ ለምሳሌ Microsoft Windows10 ያላቸው ላፕቶፖች ቀድሞ Windows Defender ይጫናሉ፡፡

ተጨማሪ የፀረ-ቫይረስ መከላከያ ማግኘት ይችላሉ: አንዳንድ ጊዜ ይህ[ነፃ](ነፃ) ነው ፣ ግን የሚከፈልባቸው ፕሮግራሞችን የሚሰጡ ኩባንያዎችም አሉ።

የቆዩ ሶፍትዌሮች ቫይረሶች ሰርገው ሊገቡባቸው የሚችሉ ቀዳዳዎች ሊኖሯቸው ይችላል፡፡ **ዝመናዎች** እነዚህ ቀዳዳዎች እንዲሞሉ ያስችላቸዋል፡፡ በደህንነትዎ ላይ ማንኛውንም ቀዳዳ ለመሙላት በራስ-ሰር ለማዘመን ፕሮግራሞችን እና ሶፍትዌሮችን ማመቻቸት ይችላሉ፡፡ ይህ ማለት እሱን ለማድረግ ማስታወስ የለብዎትም ማለት ነው፡፡ አንዳንድ ጊዜ መሣሪያውን እራስዎ ማዘመን ሊኖርብዎት ይችላል እናም እንደዚህ ከሆነ ብዙውን ጊዜ አስታዋሽ ያገኛል። እነሱን ችላ አትበሉ!

የውሂብዎን ምትኬ ያስቀምጡ

ቫይረሶች የእርስዎን ውሂብ እና መረጃ መሰረዝ ወይም መስረቅ ይችላሉ፡፡ የግል ፎቶዎችዎን ፣ ፋይሎችዎን እና መረጃዎችዎን ለመጠበቅ መሳሪያዎን ከማዘመንዎ በፊት መረጃዎን መጠባበቂያ ማድረግ አለብዎት፡፡ ምትኬ ማለት ቅጅ መፍጠር ነው ፣ ይህም ተንቀሳቃሽ ሃርድ ድራይቭን በአካላዊ ሊጠቀም ይችላል ፣ ግን ብዙውን ጊዜ ለሌላ መሣሪያ ወይም በ “ደመና” (አንላይን) ማከማቻ ውስጥ ነው። ምክንያቱም አንዳንድ ጊዜ ዝመናዎች ፋይሎችን ሊለውጡ ስለሚችሉ ነው ነገር ግን በፍጥነት መልሰው ማግኘት የሚችሉበት የመረጃዎ ምትኬ ካለዎት በራንሰምዌር ጥቃቶች ሊጠቁ አይችሉም፡፡ ራስ-ሰር ምትኬን ማብራት ይችላሉ ይህም ማለት የውሂብዎን ምትኬ ለማስቀመጥ ማስታወስ አያስፈልግዎትም ማለት ነው።

መረጃዎን ምትኬ ለማስቀመጥ ተጨማሪ መመሪያ እዚህ ይገኛል www.getsafeonline.org/protecting-your-computer/Backups

ማጠቃለያ

- ለኢሜልዎ ብቻ የተለየ የይለፍ ቃል ያኑሩ
- የኢሜል ይለፍ ቃልዎን እና ሌሎች የመለያ የይለፍ ቃሎች ጠንካራ መሆናቸውን ያረጋግጡ
- የይለፍ ቃልዎን እንዴት እንደሚለውጡ ማወቅዎን እና ይህንን በመደበኛነት ማድረግዎን ያረጋግጡ
- ለብዙ መለያዎች አንድ አይነት የይለፍ ቃል አይጠቀሙ እና የይለፍ ቃላትን ስለ መርሳት የሚያሳስብዎት ከሆነ የይለፍ ቃል አስተዳዳሪን ለመጠቀም ያስቡ፡፡
- ሁለት ደረጃ ማረጋገጫዎችን ይጠቀሙ
- ፀረ-ቫይረስ እንዳለብዎ እና እንደሚሰራ ያረጋግጡ (እና እርግጠኛ ካልሆኑ ያግኙ)

- ፀረ-ቫይረስዎን ይጠቀሙ እና ያዘምኑ - አዲስ የተገነቡ ቫይረሶችን ወይም ሳንካዎችን ለመከላከል አዘውትሮ ሙሉ ፍተሻ ያድርጉ እና ፀረ ቫይረስዎን ያዘምኑ
- ምን እንዳወረዱ ይጠንቀቁ - ማስታወቂያ ወይም ስፓይዌር ፕሮግራሞች ከሚያወርዷቸው ነገሮች ጋር እራሳቸውን በማያያዝ ኮምፒተርዎ ውስጥ ይገባሉ ስለዚህ ፋይሎችዎን ከየት እንደሚያገኙ ይፈትሹ፡፡

በአገልግሎቱ ካልረኩ ምን ማድረግ እንደሚቻል

በላፕቶፕዎ ላይ አገናኝ ከከፈቱ ወይም የሆነ ነገር ለመጫን መመሪያዎችን ከተከተሉ ግን ጥርጣሬ ካለብዎት የፀረ-ቫይረስ ሶፍትዌሩን ይክፈቱ እና ሙሉ ቅኝት ያካሂዱ፡፡ ጸረ-ቫይረሱ የሚሰጠውን ምክር በመከተል ኢንፌክሽኑን ለማስተካከል እንዲሞክር እና መሳሪያዎን መልሶ እንዲያስተካከል ይፍቀዱለት። ሊስተካከል ካልቻለ የባለሙያ እርዳታ ማግኘት ሊኖርብዎት ይችላል፡፡

የቅርብ ጓደኛዎ እርስዎን ያነጋግርዎታል እናም በጣም የተበሳጨ ይመስላል። ፎቶ ነው ብለው ባሰቡት ኢሜል ውስጥ ፋይል ከፍተዋል፡፡ ራንሰምዌር የያዘ የትሮጃን ሆርስ ነበር እናም አሁን ኮምፒውተራቸው ቆልፎባቸዋል። እርስዎ ምን ያደርጋሉ ፣ እና ምን እንዲያደርጉ ይነግራቸዋል?

በራንሰምዌርከተጠቁ እና ብሩን ለመክፈል ከመረጡ የወንጀል ድርጊቶችን እንደሚደግፍ እና መሳሪያዎን እነደሚከፍት ዋስትና እንደሌለ ይወቁ፤ እርዳታ ሳይሰጥ ሁኔታው ለወደፊቱ እንደገና ለመክፈል እና የወደፊቱን ጥቃቶች ለመጋበዝ ዝግጁ እንደሆኑ እንዲሰማዎት ሊያደርግ ይችላል።

የተለመዱ ዓይነቶች ኦንላይን ስጋት

ተንኮል እና ማጭበርበሮች

ማጭበርበር አንድን ሰው በገንዘብ ለማታለል ወይም የግል ዝርዝሮቹን እንዲሰጥ ማድረጊያ ዘዴ ነው ፣ ስለሆነም አንድ ወንጀለኛ ከሂሳቡ ላይ መስረቅ ወይም ማንነቱን መስረቅ ይችላል። ቫይረሶችን ከኮምፒውተራቸው ወይም ከኦንላይን አካውንታቸው ለመስረቅ ወይም አንድ ሰው እነሱን በማሳሳት ወይም በማታለል ገንዘብን በፈቃደኝነት እንዲያስረክብ ማድረግን ሊያካትት ይችላል፡፡

ማጭበርበር ብዙውን ጊዜ በሐሰተኛ ኢሜይሎች **(ፊሺንግ)** ፣ በፅሁፍ መልእክት **(ስሚሺንግ)** ወይም በስልክ ጥሪ **(ቪሺንግ)** በመጠቀም ይካሄዳል፡፡ ኢሜሎች ወይም ጽሑፎች የግል መረጃን ለማስገባት ወይም እንደ ኮሪዶር ሆነው ቫይረሶችን ወደ ኮምፒተርዎ እንዲፈቅድ ከሚያደርግዎ የሐሰት ድረ-ገጽ አገናኝ ሊኖራቸው ይችላል፡፡ ወይም ኢሜሉ የባንክ ዝርዝሮችን ፣ የግል መረጃዎችን ወይም ፎቶዎችን የሚሰርቅ ቫይረስ የያዘ አባሪ ሊኖረው ይችላል፡፡

ማጭበርበሮች እርስዎ ከሚያውቁት ድርጅት ወይም አንዳንድ ጊዜ እርዳታ ሚፈልግ ሰው ጋር የተገናኙ እንዲመስልዎ ያደርጋል፡፡ እርስዎ እርምጃ ለመውሰድ ፣ ብዙውን ጊዜ በፍጥነት አንድ ነገር “ለማድረግ” ግፊት እንዲሰማዎት ታስበው የተነደፉ ናቸው - አገናኝ ይክፈቱ ፣ ዝርዝሮችን ይስጡ ፣ አባሪውን ይጫኑ። አይመኑት!

ሁሉንም የማጭበርበር እና ተንኮል ዓይነቶች እዚህ ለመዘርዘር በቂ ጊዜ የለንም። ወንጀለኞች በሚጠቀሙባቸው የማጭበርበር ዓይነቶች ላይ ተጨማሪ መረጃ እንዲሁም ተንኮልን እና የሳይበር-ወንጀሎችን እንዴት ሪፖርት እንደሚያደርጉ ምክር እዚህ ይገኛል www.actionfraud.police.uk

ፊሺንግ

ፊሺንግ የማጭበርበር ዓይነት ነው ፣ አንድ የሳይበር-ወንጀለኛ ግለሰብ የግል መረጃን ፣ የባንክ ወይም የባንክ ካርድ ዝርዝሮችን ፣ ወይም የመለያ ዝርዝሮችን እና የይለፍ ቃሎችን እንዲያቀርቡ ለማባበል “መንጠቆ” ን ይጠቀማል፡፡ ከዚያ ይህን መረጃ የእርስዎን መለያዎች ለማግኘት እና ገንዘብን ለመስረቅ ወይም ከእርስዎ የኢሜል አድራሻዎችን ለመስረቅ ወይም ማንነትዎን ለመስረቅ ይጠቀማሉ። ወንጀለኞች ገንዘብን ወይም መረጃን በመስጠት ጥቂቶችን ብቻ እንደሚያታልሉ ተስፋ በማድረግ በሺዎች ለሚቆጠሩ ሰዎች የፊሺንግ ኢሜል ሊልኩላቸው ይችላል፡፡

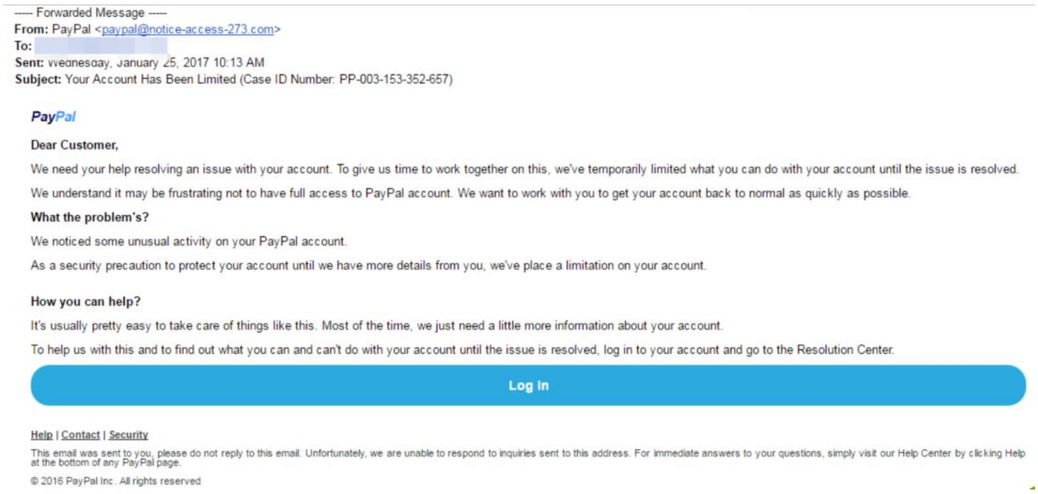
ጠላፊዎች እና አጭበርባሪዎች እርስዎ የሚያምኗቸው አንድ ሰው ወይም ድርጅት በመምሰለው ጥሩ ስራ ይሰራሉ፣ እና እንዲያውም እርስዎን ለማሳመን ለመሞከር የእርስዎን ስም እና ሌሎች የግል መረጃዎችን ሊጠቀሙ ይችላሉ። በስጦታ እርስዎን ለመሳብ ይሞክራሉ ወይም በማስፈራራት እርስዎን ለማጥመድ ይሞክራሉ። ለምሳሌ ፣ መንግስት ነኝ ብለው ሊመስሉ ይችላሉ ለምሳሌ የግብር ቢሮ ለእርስዎ ተመላሽ እንዲያደርጉልዎ ነገር ግን ለእርስዎ እንዲከፍሉ የባንክ ዝርዝርዎን እንዲያቀርቡ ሊያነጋግርዎት ይችላሉ፡፡ እርስዎ መክፈል ያለብዎት ገንዘብ እንዳለ ካልሆነ ወደ ፍርድ ቤት ትሄዳለህ ብለው የአከባቢዎ ምክር ቤት መስለው

ሊቀርቡ ይችላሉ ፣ ወይም እንደ PayPal ወይም እንደ ባንክ ወይም የባንክ አማላጅ እንደሆኑ አድርገው በማስመሰል የባንክ ሂሳብዎን ከመጠቀም ታግደዋል ሊሉ ይችላሉ፡፡

[ይህንንቪዲዮከሜትሮፖሊታንፖሊስ በፊሺንግ ላይ ይመልከቱ።](#)

በእውነት ኢሜል የላከው እና የፊሺንግ ማጭበርበሪያ መሆኑን ለመፈተሽ ፈጣን መንገድ በ "ከ" ውስጥ የሚታየውን ብቻ ሳይሆን የላኪውን የኢሜይል አድራሻ መመልከት ነው። እውነተኛ መልእክት ብዙውን ጊዜ ከሚታወቅ የድርጅት አድራሻ ይመጣል (ለምሳሌnoreply@yourbank.com) ግን አጭበርባሪዎች እና ወንጀለኞች እውነተኛውን የባንክዎን ወይም የድርጅቱን የጎራ ስም መጠቀም አይችሉም ፣ ስለሆነም ብዙ ጊዜ የኢሜል አድራሻው በዘፈቀደ ፊደሎች እና ቁጥሮች ይሞላል (ለምሳሌnoreply@1234bank12.com)። ከግል አድራሻ ከሆነ (ለምሳሌperson@gmail.com) ከኦፊሴላዊ ድርጅት የመሆን ዕድሉ አነስተኛ ነው - Google እንኳን ድርጅታዊ ኢሜሎችን ለመላክ GoogleMail (@gmail) ጎራ አይጠቀምም

ይህንን ምሳሌ ሲመለከቱ ከ PayPal እውነተኛ ኢሜይል ቢመስልም በምትኩ **ከሌላ የጎራ ስም** መሆኑን ማየት ይችላሉ: Paypal@**notice-accessxxx.com**


----- Forwarded Message -----
From: PayPal <paypal@notice-access-273.com>
To:
Sent: Wednesday, January 25, 2017 10:13 AM
Subject: Your Account Has Been Limited (Case ID Number: PP-003-153-352-657)

PayPal

Dear Customer,

We need your help resolving an issue with your account. To give us time to work together on this, we've temporarily limited what you can do with your account until the issue is resolved.

We understand it may be frustrating not to have full access to PayPal account. We want to work with you to get your account back to normal as quickly as possible.

What the problem's?

We noticed some unusual activity on your PayPal account.

As a security precaution to protect your account until we have more details from you, we've place a limitation on your account.

How you can help?

It's usually pretty easy to take care of things like this. Most of the time, we just need a little more information about your account.

To help us with this and to find out what you can and can't do with your account until the issue is resolved, log in to your account and go to the Resolution Center.

Log In

Help | Contact | Security

This email was sent to you, please do not reply to this email. Unfortunately, we are unable to respond to inquiries sent to this address. For immediate answers to your questions, simply visit our Help Center by clicking Help at the bottom of any PayPal page.

© 2016 PayPal Inc. All rights reserved

በጣም ጥሩ የሚመስሉ ወይም ትክክለኛ አርማዎች ቢጠቀሙም እና ህጋዊ ቢመስሉም ለፈጣን ውሳኔዎች የሚገፋፉ ኢሜሎችን መጠንቀቅ ተገቢ ነው፡፡ ተረጋግተው የተቀበሉትን ይጠይቁ፡፡ መልስ አይስጡ ወይም ማንኛውም አገናኞችን አይጫኑ። አንዴ አገናኙን ከከፈቱ በኋላ መረጃን ለመስረቅ በኮምፒተርዎ ላይ ቫይረሶችን ሊጫኑ ወይም ወደ ተንኮል አዘል ወይም ሀሰተኛ ድረ-ገጽ ሊዛወሩ እና ከዚያ ከእርስዎ የሚሰረቅ የሂሳብ ወይም የባንክ ዝርዝር እንዲያስገቡ ሊጠየቁ ይችላሉ፡፡

ፊሺንግ እና የማጭበርበሪያ ኢሜሎችን ማወቅ

- ላኪውን ያውቃሉ? በአጠቃላይ ሰላምታ እያነጋገሩዎት ነው?
- የፊደል አጻጻፍ ስህተቶች አሉ ወይንስ በደንብ የተፃፈ አይደለም?
- አንድ ነገር እንዲያደርግልዎት ይፈልጋል ወይም የጥድፊያ ስሜት አለ ወይንስ እያስፈራራዎት ነው?
- መልዕክቱ የተላከበትን የኢሜል አድራሻ ይክፈቱ፡፡ ትክክለኛ የጎራ ስም አለው?
- ያልታሰበ ነው ወይስ እርስዎ ከማይገናኙት ኩባንያ የተላከ ነው?
- ወደ ድረ-ገጽ የሚመራዎት ከሆነ በድረ-ገጹ ላይ ምንም የቁልፍ መቆለፊያ ምልክት እና በድር አድራሻ መጀመሪያ ላይ https: // የለም?

የፊሺንግ ኢሜሎችን ለመለየት ተጨማሪ ምክሮች እዚህ ይገኛሉ፡ www.ncsc.gov.uk

ዛህራ ከባንክዋ ነው ብላ የምታስበው ኢሜል ደርሷታል - ስትከፍተው ለጊዜው ሂሳቧን እንዳገዱት ይገልጻል፡፡ ዛህራ በፍርሃት ተውጣ ባንኩን በባንክ ሂሳቧ ላይ ያልተለመደ እንቅስቃሴ ማግኘቱን እና እሷን ለመጠበቅ ሂሳቧን ለመዝጋት መወሰኑን አወቀች፡፡ በሂሳቧ ገብታ እንደገና እንዲሰራ ካላደረገችው በስተቀር የባንክ ሂሳቡን መጠቀም እንደማትችል እና ይህን ለማድረግ አገናኝ እንድትጫን ይተይቃታል፡፡ ዛህራ ነገ የቤት ኪራይ መክፈል እንዳላት ታውቃለች ፣ እና ወዲያውኑ ሂሳቧን ማግኘት አለባት ፣ ግን ተጠራጠረች።

ዛህራ ለምክር እርስዎ ጋር ትደውልሃለች፡ ምን ይነግሯታል እና እንዴት ይመክሯታል?

አገናኙ አደገኛ ሊሆን ይችላል፡፡ ጠላፊዎች መረጃን ለመስረቅ ወይም በኢሜሏ ፣ በባንክ ወይም በማኅበራዊ ሚዲያ መለያዋ ውስጥ ሰብረው ለመግባት ለመሳሰሉ የወንጀል ምክንያቶች በኮምፒተርዋ ላይ የሆነ ነገር ለመጫን ይሞክራሉ ማለት ሊሆን ይችላል፡፡ ወይም አገናኙ መታወቂያዋን እና የይለፍ ቃሏን ወይም ሌሎች የባንክ ዝርዝሮችን ወደሚጠይቅ ሌላ ድረ-ገጽ (የሐሰት የባንክ ስሪት) ሊወስድ ይችላል፡፡ አንዴ ይህንን መረጃ ለድረ-ገጹ ከሰጠች በኋላ የባንክ አካውንቷን እና ገንዘብዋን ለአጭበርባሪዎቹ ትሰጣቸዋለች፡፡

ባንክዎ በኢሜል ፣ በስልክ ወይም በጽሑፍ አያነጋግርዎትም እና የግል ዝርዝሮችን አይጠይቅም፡፡ በእውነት የእርስዎ ባንክ እንደሚጠራዎት እና የማይረባ ማጭበርበር አለመሆኑን በጭራሽ እርግጠኛ ካልሆኑ ጥሪውን ያቋጡ እና የደንበኞቻቸውን አገልግሎት ቁጥር ኦንላይን ይፈልጉ፡፡ ተመልሰው ከመደወልዎ በፊት ለ 5 ደቂቃዎች ይቆዩ ወይም አጭበርባሪዎች የስልክ መስመሮችን መጥለፍ ስለሚችሉ የተለየ ስልክ ይጠቀሙ፡፡

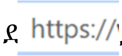
እርስዎን ካነጋገረች በኋላ፡

ዛህራ የባንኳን የደንበኞች አገልግሎት ስልክ ቁጥር ኦንላይን ትፈልጋለች፡፡ ባንኩ ይህ የውሸት ኢሜል መሆኑን አረጋግጧል እናም ሂሳቧ በትክክል እየሰራ ነው። በኢሜል ውስጥ ያለው አገናኝ የባንክ ድረ-ገጽ መስሎ ወደ ሚያሳይ ድረ-ገጽ እንደሄደ ይነግሯታል፡፡ ባንኩ ጥንቃቄ የጎደለው መሆኑን ካሳየ የዚህ ዓይነቱ የማጭበርበር ሰለባዎች አንዳንድ ጊዜ ገንዘባቸውን መልሰው ማግኘት ይቸግራቸዋል፡፡

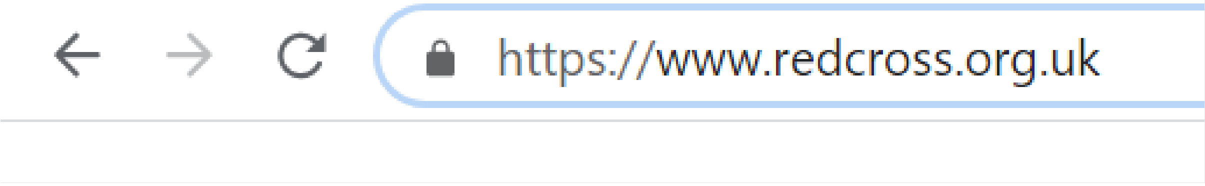
ስለፊሺንግ እና ማጭበርበሮች ተጨማሪ መረጃ በብሔራዊ የሳይበር ደህንነት ማዕከል ይገኛል ፡፡
www.ncsc.gov.uk/guidance/phishing

ደህንነታቸው የተጠበቀ እና ደህንነታቸው ያልተጠበቀ ድረ-ገጾች

የጎበኟቸው ማናቸውም ድረ-ገጾች ደህንነታቸው የተጠበቀ ስለመሆኑ ማረጋገጥ መቻል አስፈላጊ ነው፡፡ የጎበኙት ማንኛውም ድረ-ገጽ ደህንነቱ የተጠበቀ ላይሆን ይችላል ፣ ወይም የሐሰት ኢሜሎችን የሚልክልዎት ጠላፊዎች በጣም እውነተኛ ወደሚመስል የውሸት ድረ-ገጽ ሊያዞሩዎት ይችላሉ፡፡

ይህንን የፓድሎክ አርማ ወይም በአሳሽ ባር ውስጥ እነዚህን ደ 

ይፈልጉ ይህም አንድ ድረ-ገጽ ደህንነቱ የተጠበቀ ነው ማለት ነው።



አንዳንድ ጊዜ በኮምፒተር ወይም በአሳሽ ላይ በመመርኮዝ ሁለቱንም **ፓድሎክ** እና **https** ወይም የፓድሎክ ምልክትን ብቻ ያያሉ፡፡ ‘S’ ደህንነቱ የተጠበቀ መሆኑን የሚያመለክት ስለሆነ **https** ብቻ ያለው ድረ-ገጽ ደህንነቱ የተጠበቀ ላይሆን ይችላል።

ወደ አንድ ሂሳብ እንዲገቡ ፣ የክፍያ ዝርዝሮችን ወይም ሌላ መረጃ እንዲያቀርቡ ከተጠየቁ የሚጠቀሙባቸው ማንኛውም ድረ-ገጾች በአሳሹ ባር ውስጥ በአድራሻው መጀመሪያ ላይ “https” እንዳለው ያረጋግጡ። ትክክለኛውን የድረ-ገጽ አድራሻ መሆኑን እና ደህንነቱ የተጠበቀ መሆኑን ሲረዱ ብቻ በመለያዎች ዝርዝር ውስጥ ይግቡ፡፡

የባንክዎን ድረ-ገጽ ለመጎብኘት ሁል ጊዜ ሙሉ የድር አድራሻውን ይተይቡ በተለይም ወደ ኦንላይን ባንክ የሚገቡ ከሆነ፡፡ ወደ ባንክዎ ድረ-ገጽ ለመግባት በጭራሽ የፍለጋ ሞተርን አይጠቀሙ ፣ ምክንያቱም ይህ እርምጃ ጠላፊዎች ደህንነትን ለማበላሸት እና ዝርዝርዎን ለመስረቅ ሊጠቀሙበት ስለሚችሉ ነው።

በፊሺን እና በማጭበርበር ድረ-ገጾች ላይ እርምጃ ይውሰዱ

ራስዎን ለመጠበቅ ለመሞከር የሚከተሉትን ምክሮች ያስታውሱ፡

- የአሳሽዎን ሶፍትዌር ፣ ጸረ-ቫይረስ እና ስፓይዌሮችን ወቅታዊ ያድርጉ
- ደህንነታቸው ያልተጠበቀ ወይም ፓድሎክ የሌላቸውን አደገኛ ድረ-ገጾችን ያስወግዱ
- ከማይታወቅ ወይም አጠራጣሪ ምንጭ በሆነ ኢሜይል ውስጥ የሚገኝ አገናኝ በጭራሽ አይጫኑ
- የግል ዝርዝሮችዎን ፣ የይለፍ ቃላትዎን ወይም የደህንነት ኮዶችዎን በኢሜል ወይም በስልክ በጭራሽ አይስጡ

በማጭበርበር ከተጠቁ ምን ማድረግ ይኖርብዎታል

ኢሜሉን ፣ ጥሪውን ፣ መልዕክቱን ወይም ድረ-ገጹን ሪፖርት ያድርጉ፡፡

ኢሜል ከተቀበሉ እና እርግጠኛ ካልሆኑ በ report@phishing.gov.ukወደ**አጠራጣሪ የኢሜይል ሪፖርት አገልግሎት (SERS)**ማስተላለፍ ይችላሉ።የፊሺንግ ኢሜይል ከሆነ ወይም እንደ ሆነ ይነግራሉ።

አጠራጣሪ የጽሑፍ መልእክት ከተቀበሉ በነጻ ወደ 7726 መላክ ይችላሉ፡፡ የስልክ አቅራቢዎ ጽሑፉን እንዲመረምር እና ማጭበርበር ከሆነ እርምጃ እንዲወስድ ያስችለዋል፡፡

ዝርዝሮችዎን አያጋሩ ግን ይልቁንስ ይፈትሹ፡፡ በኢሜል ውስጥ ያለውን ቁጥር በጭራሽ አይደውሉ ወይም አገናኞቹን አይጫኑ ወደ ሌላ የሐሰት መለያ ሊያመሩዎት ስለሚችሉ፡፡ ኦንላይን ይሂዱ እና በሰፊው የሚተዋወቀውን ቁጥር ያግኙ እና ይልቁንስ ይደውሉ።

የት እንደሚወስዱዎት ሳይጠይቁ አገናኞችን አይከተሉ። አንድ ድረ-ገጽ እውነተኛ መሆኑን ለመፈተሽ የድር አሳሽዎን ይክፈቱ እና ስሙን በ URL ባር ውስጥ በመተየብ በቀጥታ ይሂዱ።

የይለፍ ቃልዎን ወይም የፒን ቁጥርዎን በጭራሽ አያጋሩ። የሚጠይቀው ሰው እናትዎ ወይም የቅርብ ጓደኛዎ ነው ብለው ቢያስቡ እንኳን - የይለፍ ቃልዎን አይስጡ፡፡

የባንክ ዝርዝር መረጃዎችን እንዲያቀርቡ ከታለሉ አንድ ጊዜ ለባንክዎ ይንገሩ፡፡

ገንዘብ ከጠፋብዎት ለባንክዎ ይንገሩ እና**ለማጭበርበርድርጊት(Action Fraud)**(ለእንግሊዝ ፣ ለዌልታ እና ለሰሜን አየርላንድ) ወይም **ለፖሊስ ስኮትላንድ** (ለስኮትላንድ) ሪፖርት ያድርጉ ይህንን በማድረጉ ሌሎች እንዲሁ ተጠቂዎች እንዳይሆኑ ለመከላከል ይረዳሉ፡፡

የማጭበርበር ድርጊት www.actionfraud.police.uk

ኦንላይን ግንኙነቶች

በዚህ ክፍል ውስጥ ኢንተርኔት በግል ግንኙነቶች ውስጥ ስላለው ተፅእኖ እንነጋገራለን፡፡ ኦንላይን የምናደርገው ነገር በቀጥታ በግል ሕይወታችን ላይ ተጽዕኖ ሊያሳድር ይችላል፡፡ ስለሆነም ኦንላይን ለሌሎች ሰዎች ስለሚያጋሯቸው መረጃዎች በጣም ጠንቃቃ መሆን አስፈላጊ ነው፡፡

ሁላችንም ከሰዎች ጋር መገናኘት እንፈልጋለን ፣ እናም በዓለም ዙሪያ ከጓደኞቻችን ፣ ከቤተሰቦቻችን እና የጋራ ፍላጎት ካላቸው ሰዎች ጋር በቀላሉ መገናኘት የምንችልበት ምርጥ ነገሮች አንዱ ነው። በተመሳሳይ ጊዜ ኦንላይን ያሉ ግንኙነቶች በመንገድ ላይ ካለ

ሰው ጋር እንደሚገናኙ ሁሉ በጥንቃቄ መምራት እንደሚገባቸው እና ሌሎች ወደ መጥፎ ድርጊት የሚወስድ መጥፎ እምነት ካላቸው ሰዎች ጋር ጋር ግኑኝነትን መፍጠር ይፈልጋሉ።

ኦንላይን በደል ሙሉ ለሙሉ ከማያውቋቸው ሰዎች ወይም ቀድሞውኑ ከሚያውቋቸው ሰዎች ሊሆን ይችላል ፣ እና ከዚህ በታች ኦንላይን የግለሰቦች ግላዊ ጥቃት አንዳንድ ምሳሌዎችን እንመለከታለን።

የፍቅር ስሜት ማጭበርበር

የፍቅር ማጭበርበር ማለት አንድ ሰው ኦንላይን የፍቅር ግንኙነት ድረ-ገጽ ወይም መተግበሪያን በመጠቀም ፣ መተማመንን ለማግኘት እና ከዚያ ገንዘብ ወይም የግል መረጃን ለመጠየቅ የግለሰቦችን የግል ግንኙነት ሲያዳብር ነው። እነሱ ግንኙነታቸውን ለመመሥረት የሐሰት መገለጫን የሚጠቀሙ ይሆናል ፣ እናም እውነተኛ እና አሳቢ መስለው ሊታዩ ይችላሉ። በጣም ብዙ ጊዜ ይህ ሰው ብዙ የግል ጥያቄዎችን ይጠይቃል ፣ ግን ስለራሱ ብዙ አያሳይም ወይም አይናገርም፡፡ እነሱ እምነት እንዳዳበሩ እርግጠኛ እስኪሆኑ ድረስ ይተብቁ እና አብዛኛውን ጊዜ ገንዘብን ለመጠየቅ ስሜታዊ ትስስርን ይጠቀማሉ ፣ ግን አብዛኛውን ጊዜ ጥቅል መቀበል ወይም አድራሻ መስጠት ሊሆን ይችላል። ብዙውን ጊዜ ኢንተርኔት ላይ ሌላ ቦታ የተነሱ የሐሰት ሥዕሎችን ወይም የራሳቸውን ፎቶግራፎች ሊልኩ ይችላሉ፡፡

ምንም ያህል ቢተማመኑም ወይም ታሪካቸውን ቢያምኑም ገንዘብ በጭራሽ አይላኩ ወይም አይቀበሉ ወይም የባንክ ዝርዝርዎን ኦንላይን ለሚያገኗቸው ሰው **በፍጹም** አይስጡ፡፡

ኦንላይን ልዩ ወዳጅነት ወይም ግንኙነት ፈጥረዋል ብሎ በማሰብ መታለል በእውነቱ ቅር ሊያሰኝ ወይም አሳፋሪ ሊሆን ይችላል ፣ ግን ለ የማጭበርበር ድርጊት ጋር ሪፖርት ማድረግ ወይም በ 0300 123 2040 መደወል ይችላሉ፡፡

የአንድን ምስል ምንጭ ለመፈተሽ *የተገላቢጦሽ የምስል ፍለጋ* ማድረግ ይችላሉ ፣ ስሙ እንደሚለው እንደነዚህ ያሉትን ሌሎች ለማግኘት በኢንተርኔት ምስሎች ውስጥ ይፈልጉዎታል፡፡ የተገላቢጦሽ የምስል ፍተሻ እዚህ ማድረግ ይችላሉ

የሳይበር ጉልበተኝነት

የሳይበር ጉልበተኝነት ኦንላይን ወይም ቴክኖሎጂን በመጠቀም ጉልበተኝነት እና ትንኮሳ አጠቃላይ ቃል ነው፡፡ በሌላ ሰው ላይ ጉዳት ፣ ጭንቀት ወይም የግል ኪሳራ ለማምጣት የታቀደ ማንኛውንም ዓይነት የኦንላይን በደል ይሸፍናል፡፡ ብዙውን ጊዜ ጉልበተኞች እንደ ፌስቡክ (Facebook) ወይም ትዊተር (Twitter)፣ መልእክት መላላኪያ ወይም በይነተገናኝ መድረኮች ያሉ ማህበራዊ ሚዲያ አውታረመረቦችን ይጠቀማሉ፡፡ የሳይበር ጉልበተኝነት በተለይ በትምህርት ቤት ወይም በሥራ ባሉ ልዩ ሁኔታዎች ብቻ ሳይሆን በኢንተርኔት እና በሞባይል ስልኮች በማንኛውም ጊዜ ሰዎችን ማግኘት ስለሚችል በጣምአስጨናቂሊሆንይችላል፡፡

አንድ ሰው በኢንተርኔት ወይም በማህበራዊ አውታረመረቦች ላይ ስለእርስዎ ሀሰተኛ ወይም ተንኮል-አዘል ነገሮችን ከለጠፈ እንደ ትንኮሳ ተደርጎ ሊወሰድ ይችላል ይህም ወንጀል ነው፡፡ እንደዚሁም ፣ እርስዎን የሚያስፈራራዎት ጥሪዎች ከተቀበሉ ደዋዩ ወንጀል እየፈጸመ ነው፡፡

ጉልበተኝነት ሕፃናትንም ሆነ ጎልማሶችን ጨምሮ ማንንም ሊነካ ይችላል ፣ ነገር ግን የልጆች ወላጅ ወይም ተንከባካቢ መሆንዎን ማወቅ በጣም አስፈላጊ ነው፡፡ እርስዎ ወይም ልጅዎ ወይም አንድ የምታውቁት ሰው ኦንላይን ጉልበተኝነትን ጨምሮ ጥቃት የሚሰነዝሩ ከሆነ በ 0300 323 0169 ላይ ምክር ለማግኘት ለ ብሔራዊ ጉልበተኛ እርዳታ መስመር መደወል ይችላሉ፡፡

ማባበል

ማባበል ማለት አንድ ሰው ብዝበዛን እና መቆጣጠር እንዲችል ከአንድ ሰው ጋር የግንኙነት መተማመን እና ግንኙነት ሲገነባ ነው፡፡ ለአካለ መጠን ያልደረሰ ልጅ ለወሲባዊ ጥቃት (ኦንላይን ወይም በአካል) ፣ ለአደንዛዥ ዕፅ ማዘዋወር ወይም ለሌላ የብዝበዛ ዓላማ ሲባል ኦንላይን የልጆችን እና ወጣቶችን ማባበል በጣም አሳሳቢ ነው፡፡

ማባበል በአጭር ወይም ረጅም ጊዜ ውስጥ ሊከናወን ይችላል እናም የሚያባብሉ ሰዎች ከልጁ ቤተሰቦች ጋር እምነት የሚጣልባቸው ፣ ስልጣን ያላቸው እና አጋዥ እንዲመስሉ ግንኙነታቸውን ሊገነቡ ይችላሉ፡፡ ዘር ፣ ጾታ ፣ ዕድሜ ወይም ከልጁ ጋር ያለው ግንኙነት ምንም ይሁን ምን ማንኛውም ሰው የሚያባብል ሰው ሊሆን ይችላል።

የሚያባብል ሰው እራሱን እንደ እኩያ ለልጁ ሊያቀርብ እና ይህንን የሚደግፉ የሌሎች ሰዎችን ፎቶዎችን ወይም ቪዲዮዎችን በሚልክበት ኦንላይን ሊከናወን ይችላል፡፡ ታማኝ ለመምሰል ጨዋታዎችን መጫወት ፣ ምክር መስጠት ፣ ማስተዋል ማሳየት እና ለወጣቱ ስጦታዎች ሊገዙ ይችላሉ ፣ ወይም ልጁን ከቤተሰብ ወይም ከጓደኞች ለማግለል ይሞክራሉ ፣ አንድን ልጅ በድርጊት ወይም በተግባር ባለማሳየት ለመሞከር እና ለማሸማቀቅ ብላክሜል ይጠቀማሉ ፣ ወይም ልጁን ለመቆጣጠር “ሚስጥሮች” የሚለውን ሀሳብ ያመጣሉ።

ስለማባበል ተጨማሪ መረጃ, ሕፃናትን ስለ ኦንላይን ማስፈራሪያዎች እንዴት ማውራት እንደሚቻል የሚያብራሩ ከሌሎች ሀብቶች ጋር በ NSPCC ድረ-ገጽ ይገኛል:: www.nspcc.org.uk

ልጅ አደጋ ላይ ነው ብለው ከጠረጠሩ ለፖሊስ ከመናገር ወደኋላ አይበሉ:: እንዲሁም ኦንላይን የሚፈጸመውን በደል ሪፖርት ለማድረግ እና ምክር ለማግኘት NSPCCን ማነጋገር ይችላሉ።

ሴክስቲንግ እና የበቀል የወሲብ ስራ

ሴክስቲንግ የወሲብ መልእክት ፣ ፎቶ ወይም ቪዲዮ ለሌላ ሰው ሲላክ ነው:: አንድ ሰው የራሳቸውን ወይም የሌላ ሰው ምስል ሊልክ ይችላል:: አንድ **ሴክስት** ለጓደኛዎ ፣ ለባልደረባዎ ወይም ለሌላ ሰው ኦንላይን ሊሆን ይችላል ፣ እና ከፊል ወይም ሙሉ እርቃን፣ ወሲባዊ ግልጽ በሆነ መንገድ መቅረጽ ወይም ስለ ወሲባዊ ድርጊቶች ማውራትን ሊያካትት ይችላል።

ወሲባዊ መልእክት በሁለት ስምምነት ባላቸው ወገኖች መካከል መላክ ቢቻልም ፣ምስሎች ያለባለቤቱ ስምምነት በኢንተርኔት በፍጥነት ሊጋሩ ይችላሉ:: የሆነ ሰው ኦንላይን አንድ ምስል ወይም ቪዲዮ ከተጋራ በኋላ ለማንም ሰው መላክ ይችላሉ።

የበቀል ወሲብ ማለት አንድ ሰው **ጭንቀት ለመፍጠር በማሰብ** ያለባለቤቱ ፈቃድ **የግል ወሲባዊ** ፎቶግራፍ ወይም ፊልም ለሌላ ሰው ወይም ሰዎች ሲያሳይ ወይም ሲያሳትም ነው::

አንድን ሰው የግል መረጃውን እና ፎቶግራፎቹን በመግለጥ ማስፈራራት እንዲሁ ብላክሜል እና የወንጀል ጥፋት ነው:: በበቀል ወሲብ ላይ ተጨማሪ መረጃ እዚህ ይገኛል

የበቀል የወሲብ እገዛ መስመር - 0845 6000 459

www.revengepornhelpline.org.uk/

አንድ ሰው እርቃናቸውን ስዕሎች እንዲልክ ሌላ ሰው ላይ ጫና ማድረጉ በጭራሽ ጥሩ አይደለም::

እንደ Snapchat ያሉ አገልግሎቶችን እንኳን የተላኩ ምስሎች አሁንም በቅጽበታዊ ገጽ እይታ (ስክሪንሾት) ሊደረጉ እና ሊቀመጡ እንደሚችሉ ማስታወሱ አስፈላጊ ነው:: እርቃን ወይም ወሲባዊ ምስልን ከላኩ እና ምን ሊሆን ይችላል የሚል ስጋት ካለብዎት በእነዚህ ምክሮች አማካይነት እርምጃ መውሰድ ይችላሉ፡

- መልዕክቱ እንዲሰረዝ ይጠይቁ።
- ለማስፈራራት መልስ አይስጡ::
- ሰው ጋር ይነጋገሩ እና ድጋፍ ይጠይቁ። የበቀል የወሲብ እገዛ መስመርን ማነጋገር ይችላሉ።
- **የሆነውን ሪፖርት ያድርጉ::** ምስሎቹ በሚታተሙበት ድረ-ገጽያ ላይ የተሳሳተ ይዘት ሪፖርት ማድረግ ይችላሉ። አብዛኛዎቹ የማህበራዊ ሚዲያ መድረኮች ይዘትን ሪፖርት የሚያደርጉበት መሳሪያ አላቸው:: እንዲሁም እንደዚህ ዓይነቱን ወከባ ለፖሊስ ማሳወቅ አለብዎት: ድንገተኛ ካልሆነ ወደ 101 ይደውሉ::

በ 2003 በወሲብ ጥፋቶች ሕግ መሠረት **ዕድሜው ከ 18 ዓመት በታች** የሆነን እርቃን ምስል ማጋራት በልጆች ላይ የሚፈጸሙ በደሎች እና ወንጀል እንደሆነ ማወቅ አስፈላጊ ነው። እንደ ዕድሜው ከ 18 ዓመት በታች የሆነ ሰው 'ሴክስት' ላይ ማለፉ የፖሊስ ምርመራን ያስከትላል።

ስለ ልጆች የሚጋሩ ምስሎች የሚጨነቁ ከሆነ ወይም ኦንላይን ስለ ልጅ ጥበቃ የሚያሳስብዎት ሌሎች ጉዳዮች ካሉ እነዚህን ለህፃናት ብዝበዛ እና ኦንላይን የጥበቃ ማዕከል ማመልከት ይችላሉ:: www.ceop.police.uk

የሳይበር ክትትል እና ቁጥጥር

ክትትል ከሌላው ሰው የሚመጣ የባህሪ ዘይቤ ነው ፣ ይህም ጥቃት ይደርስብኛል የሚል ፍርሀት የሚሳድርብዎት ወይም ድንጋጤ የሚፈጥርብዎ እንዲሁም በተለመደው የዕለት ተዕለት እንቅስቃሴዎ ላይ ከፍተኛ ተጽዕኖ ያሳድራል:: ኦንላይን ሲከናወን የሳይበርክትትል ይባላል:: በእርስዎ ላይ መረጃ መሰብሰብ ፣ እርስዎን መምሰል ፣ አላስፈላጊ ወይም ማስፈራሪያ መልዕክቶችን መላክ ፣ እርስዎን መከታተል ወይም ወደ የኦንላይን መለያዎን ማግኘት እና ስለእርስዎ የተሳሳተ መረጃን ማሰራጨት ሊሆን ይችላል:: የሚከታተል ሰው የሚያውቁት ወይም እንግዳ ሰ የሆነ ሰው ሊሆን ይችላል። የሳይበርክትትል በተጠቂው ላይ ከባድ ተጽዕኖ ሊያሳድር ስለሚችል የወንጀል ጥፋት ነው።

ብሔራዊ የክትትል የእገዛ መስመር - 0808 802 0300

www.stalkinghelpline.org/faq/about-the-law/

በጥቃት አድራሻ እየተከታተልዎ ወይም እየተመለከተዎት ነው የሚል ስጋት ካለዎት:

- ብዙውን ጊዜ ከእርስዎ ጋር ለመነጋገር እና ግንኙነት ለመመሥረት ከሚፈልግ የሚከታተል ሰው ጋር ከመሳተፍ ይቆጠቡ:: እነሱን ለመገናኘት በጭራሽ አይስማሙ እና አይጋፈጧቸው::
- በቁም ነገር ይያዙት እና እንቅስቃሴውን ለፖሊስ ያሳውቁ:: በቀጥታ ለፖሊስ ለማነጋገር ወደ 101 መደወል ይችላሉ ነገር ግን ወዲያውኑ የስጋት ጥሪ አለ ብለው ካሰቡ 999 ይደውሉ::
- የግላዊነት ቅንብሮችዎን ያረጋግጡ ፣ ኦንላይን ስለእርስዎ አነስተኛ መረጃ መገኘቱን ያረጋግጡ ፣ እና በመሣሪያዎ ላይ የአካባቢ ማሳወቂያ ያጥፉ።
- በአካባቢዎ ያሉ ሰዎችን ያሳውቁ:: ስለእርስዎ ምን እያጋሩ እንደሆኑ መፈተሽ ሊያስፈልጋቸው ይችላል እንዲሁም የግላዊነት ቅንብሮቻቸውን ማረጋገጥም ይፈልጉ ይሆናል::
- ምን እንደሚከሰት መዝገብ ይያዙ - ጥሪዎች ፣ መልዕክቶች ወይም የማኅበራዊ ሚዲያ ልጥፎችን ስክሪንሾት ያድርጉ ፣ ይህም ማለት አጥቂው በኋላ መልእክቶቻቸውን እና ልጥፎቻቸውን ቢሰርዝም እንኳ የማስረጃው ቅጅ አለዎት ማለት ነው::

የቤት ውስጥ ጥቃት ፣ ትንኮሳ እና ክትትል

ጥቃት አድራሽ ተጎጂን ለመመልከት ፣ ለመፈተሽ እና ለመቆጣጠር ኢንተርኔት ያለው መሣሪያ ባህሪያትን አላግባብ ሊጠቀም ይችላል:: ይህ ከሌሎች ሰዎች ጋር ያለዎትን ግንኙነት መከታተል ፣ በመሣሪያዎ በኩል ያለዎትን ቦታ መከታተል ወይም የገንዘብ ወጪዎን መመርመርን ሊያካትት ይችላል። እነዚህ ባህሪዎች በባልደረባ ፣ በቀድሞ አጋር ፣ በቤተሰብ አባል ወይም በአሳዳጊ ሲፈፀሙ ሁሉም በ UK ህግ መሰረት የቤት ውስጥ ጥቃት ዓይነቶች ተደርገው ይወሰዳሉ::

አንድ ሰው ተንቀሳቃሽ ስልክዎን ወይም ሌላ ማንኛውንም መሳሪያ እየተከታተለ ሊሆን ይችላል የሚል ስጋት ካለብዎ ብሄራዊ የቤት ውስጥ ጥቃት የእገዛ መስመር ደህንነቱ የተጠበቀ እንዲሆን ቅንብሮችን ለመቀየር የሚያግዝዎ የሚያሳይ መሳሪያ አለው::
ብሔራዊ የቤት ውስጥ ጥቃት የእገዛ መስመር (24 ሰዓት) 0808 220 0247

www.nationaldomesticviolencehelpline.org.uk

በሚቀጥሉት መግለጫዎች ትስማማለህ?

የኦንላይን ማስፈራሪያዎች በእውነቱ ምንም አይሆኑም ምክንያቱም 'እውነተኛው' ዓለም አይደለም

አይ:: ኦንላይን የሚፈጸሙ ጥቃቶች ከባድ ፣ በሰዎች ሕይወት ላይ ከፍተኛ ተጽዕኖ የሚያሳድሩ እና ሁልጊዜም በባለሥልጣኖች በቁም ነገር መታየት አለባቸው:: መከታተል ፣ መቆጣጠር እና ትንኮሳ ሁሉም የእርስዎ ስህተት ያልሆኑ ከፍተኛ ተጋላጭነት ባህሪዎች ናቸው:: ሪፖርት የማድረግ ፣ ምክርን የመጠየቅ እና እሱን ለመፍታት ድጋፍ የማግኘት መብት አለዎት::

የትንኮሳ ወንጀል በእውነተኛ ህይወት ውስጥ በአመፅ ማስፈራራት ማለት ነው::

ሕጉ እንደሚናገረው ትንኮሳ አንድ ሰው ለእርስዎ ጭንቀት ወይም አስደንጋጭ ነገር ሊያደርሰዎት በሚችል መንገድ ሲሠራ እና ባህሪው ከአንድ ጊዜ በላይ በሚከሰትበት ጊዜ ነው:: በተለያዩ አጋጣሚዎች ወይም ሁኔታዎች የተለያዩ የባህሪ ዓይነቶች ሊሆኑ ይችላሉ:: ለምሳሌ ፣ እርስዎን ለማስጨነቅ የታሰበ አንድ መልእክት ትንኮሳ አይደለም:: ሁለት መልዕክቶች ትንኮሳ ሊሆኑ ይችላሉ ፣ ወይም በማስፈራሪያ ኢሜል የተከተለ የስልክ ጥሪ ትንኮሳ ሊሆን ይችላል:: ሌሎች እንደ ትንኮሳ የሚቆጠሯቸው ተግባራት እርስዎ ተከታትለው ከሆነ ፣ ቤትዎ ወይም ሥራዎ እየታየ ከሆነ ፣ ንብረትዎ የተበላሸ ከሆነ ወይም ምንም ስህተት ባልፈፀሙ ጊዜ በተንኮል እና በሐሰት ለፖሊስ ሪፖርት ከተደረጉ ሊሆኑ ይችላሉ::

ዛህራ በጣም የምትቀራረብ የአጎት ልጅ አላት:: የአጎቷ ልጅ ሰምኑን ትበሳጫለች ፣ ትነጫነጫለች እና ሁል ጊዜ አብረው በሚሆኑበት ጊዜ ሁሉ ስልኳን በፍርሃት እያየች የተለየ ሰው ሆናለች:: በመጨረሻም የዛህራ የአጎት ልጅ የተለያየችው የቀድሞ ባሏ በሚያደርስባት ማስፈራሪያ እንደማትተኛ እና እንደምትጨነቅ ትነግራታለች:: ዘወትር መልእክቶችን ይልክላት እና እሷ በጣም

መጥፎ ሚስት እንደሆነች ፣ እና ለሁለቱም ቤተሰቦቻቸው እፍረት እንዳመጣች እና እሷም ተመልሳ አብዋው መኖር እንዳለባት ኢሜሎችን ይልክላቸዋል፡፡ የዛህራ የአጎት ልጅ ይህንን ስታወራ በጣም ተጨንቃለች፡፡

የቀድሞ ባሏ ግንኙነታቸው ጤናማ በነበረበት ጊዜ አብረው የወሰዱትን እርቃናቸውን የሚያሳይ ፎቶግራፍ እንዳለውም ታስረዳለች፡፡ ወደእሱ ካልተመለሰች እርቃናቸውን የተነሱትን ፎቶ ወደ ቤተሰቦቿ እንደሚልክ ዝቷል፡፡

የዛህራ ዘመድ የወንጀል ሰለባ ነች?

አዎ፡፡ የዛህራ ዘመድ **የትንኮሳ እና የግዴታ ቁጥጥር** ሰለባ ነች። እነዚህ ዛቻዎች በዛራ የአጎት ልጅ ላይ የተደረጉ ሲሆን በእሷ ላይ ቁጥጥር ለማድረግ ለመሞከር የተደረጉ ናቸው፡፡ ሕጉ ይህ ጥፋት አንድ ሰው ጭንቀት ወይም አስደንጋጭ ነገር ሊያመጣብዎት በሚታሰብበት መንገድ ሲሠራ ነው ይላል፡፡ ባህሪው ከአንድ ጊዜ በላይ መሆን አለበት፡፡

ይህ ባህሪ በቀድሞ ባሏ የተደረገ እንደመሆኑ ይህ ትንኮሳ **የማስገደድ ቁጥጥር(የቤት ውስጥ ጥቃት** ዓይነት) ነው፡፡ የወንጀል ጥፋት ነው፡፡ ይህንን ለፖሊስ ማሳወቅ አለባት፡፡

እንዲሁም ጭንቀት ወይም ውርደት ለመፍጠር በማሰብ የግል ወሲባዊ ምስሎቿን ያለፍቃድ ማጋራት የበቀል የወሲብ ሥጋት ነው፡፡ ዛቻው በራሱ ጥፋትን አያስከትልም ፣ ሆኖም የዛህራ የቀድሞ ባል ይህንን ምስል ኦንላይን ፣ በዋትስአፐ ወይም ሌሎች የመልዕክት አገልግሎቶችን ጨምሮ በኢሜል ወይም በማኅበራዊ አውታረመረቦች አማካይነት ቢያካፍል ይህ ጥፋት ይሆናል።

የዛህራ ባል እንዲሁ ስለቤተሰብ ክብር እና ስለ መለያየታቸው በቤተሰቡ ላይ 'እፍረትን' እንደሚያመጣ ይናገራል፡፡ 'ክብር' ተብሎ የሚጠራው ዓመጽ የጥቃት ዓይነት ነው እናም ዛህራ በክብር ላይ ከተመሠረቱ ጥቃቶች እና ዛቻዎች ሰለባዎች ጋር አብሮ ከሚሠራው ድርጅት ድጋፍ ማግኘት ትፈልግ ይሆናል፡፡ **Karma Nirvana** ከሰኞ እስከ አርብ በ 0800 5999 247 የስልክ ድጋፍ መስመር አለው www.karmanirvana.org.uk

ማጠቃለያ

- ከመለጠፍዎ በፊት ያስቡ፡፡ ነገሮች ወደ የተሳሳተ እጅ ቢገቡ ምን እንደሚሰማዎት ከግምት ሳያስገቡ ነገሮችን አይጫኑ ወይም አይጋሩ፡፡ አንዴ አንድ ነገር ከለጠፉ መቆጣጠር አይችሉም ፣ በተለይም ሌላ ሰው ስክሪንሾት ከወሰደ፡፡
- ማንነትዎን ይጠብቁ እና በማህበራዊ አውታረመረቦች ላይ ሁሉንም ነገር አያጋሩ። ማህበራዊ ሚዲያዎች ከጓደኞች እና ቤተሰቦች ጋር ለመገናኘት በጣም ጥሩ ነገር ነው ነገር ግን እርስዎ ካሰቡት በላይ ስለ ሕይወትዎ የበለጠ ለዓለም እየተናገሩ እንደሆነ ያስቡ፡፡
- ኦንላይን የሚያጋሩትን ማን ማየት እንደሚችል በጥንቃቄ ያስቡ ፣ የግላዊነት ቅንብሮችዎ ወደ ከፍተኛ ደረጃ እንደተዘጋጁ ይፈትሹ እና ከማን ጋር እየተነጋገሩ እንደሆነ ያስቡ፡፡
- ስለማጭበርበሮች ምልክቶች እና እንዴት የማጭበርበሪያ ኢሜሎችን እና ድረ-ገጾችን ለመፈለግ ይጠንቀቁ
- እንደ አድራሻዎ ፣ ስልክ ቁጥርዎ ፣ ሙሉ ስምዎ እና የትውልድ ቀንዎ ያሉ በጣም የግል መረጃዎችን ኦንላይን በጭራሽ አያውጡ።
- በዝርዝሮች እና በይለፍ ቃላት ውስጥ መዝገብዎን በጭራሽ አይስጡ፡፡
- የማይታወቁ ኢሜሎችን ፣ ፋይሎችን ወይም አባሪዎችን በጭራሽ አይክፈቱ እና ስለፊሺንግ እና ማጭበርበሮች ይወቁ