ህዝባዊ Wi-Fi ሲጠቀሙ ደህንነትዎን ለማስጠበቅ የሚረዱ ምክሮች

መልካም ያልሆነ አላማ ያላቸው ሰዎች ኦንላይል አርሶን ሊያጠቁ ይችላሉ። ህዝባዊ Wi-Fi መጠቀም ካለብዎ ከዚህ በታች ያሉትን ምክሮች ያንብቡ።

ከኮሮና ቫይረስ ወረርሺኝ ምላሽ፣ የንግዶች እና ቤተመጽሀፍት መዘጋት ጋር በተያያዘ እብዛኛዎቻችን ኦንላይን ጊዜ እያጠፋን እንገኛለን። በዚህም ምክንያት ህዝባዊ Wi-Fi በመጠቀም ኢንተርኔት ለመጠቀም ያስፈልገን ይሆናል። ህዝባዊ Wi-Fi ለመጠቀም የግድ ሆኖቦት ራስዎን የሚያገኙ ከሆነ እባክዎ የሚከተሉትን ምክሮች ከግምት ውስጥ ያስገቡ፣ ይህም ውሂብዎን ለመጠበቅ ይችሉ ዘንድ የሚያስችል ከክልሉ ዋና የግለኝነት መኮንን የወጣ መረጃ ነው:

1. ትክክለናው አውታረመረብ እንዳለ ያረጋግጡ።

ከትክክለኛው አውታረ መረብ ጋር እንደተገናኙ እርግጠኛ ይሁኑ። መልካም አላማ የሌላቸው ሰዎች ጉዳት የማያስከትል የሚመስል አውታረ መረብ በስማቸው ሊፈጥሩ የሚችሉ ሲሆን እውነታው ግን የኢንተርኔት እንቅስቃሴዎትን ለማየት የሚያስችል የአውታረመረብ ግንኙነት ውስጥ እንዲገቡ የሚያደርግ ነው። ይህም ማለት የመግቢያ መረጃዎችን እና የይለፍቃሎችን የሚያስገቡ ከሆነ፣ ጠላፊው መረጃዎትን ሊስርቅብዎ ይችላል ማለት ነው። ራስዎን ከዚህ ለመጠበቅ፣ የአውታረመረቡን ስም በጥንቃቄ ያንብቡ፣ የሚቻል ከሆነ ደግሞ እዚህ ቦታ ላይ ያለውን ሰራተኛ ምልክቱ ልክ መሆኑን እንዲያረጋግጥልዎ ያድርጉ፣ ምክንያቱም አውታረመረቡ ትክክለኛ መሆኑን ለማረጋገጥ የሚያስችልዎ ስለሆነ ነው።

እውቅና ያላቸው አውታረመረቦች፣ ማለትም እንደ ካፍቴሪያዎች ውስጠ ያሉት፣ አጠራጣሪ ላይሆኑ ይችላሉ፣ ምክንያቱም ደግሞ ድርጅቱ አውታረመረቡን የሚያቀርበው እንደ አገልግሎቱ አካል ስለሆነ ነው። የሚታወቁ አውታረመረቦች በጠቅላላው ከ ማይታወቁ በስልክዎ ላይ ብቅ ከሚሉ Wi-Fi አውታረመረቦች ደህንነታቸው አስተማማኝ የሆነ ነው።

2. በራስ አገናኝን ያጥፉ።

ብዙ መሳሪያዎች (ስማርትስልኮች፣ ላፕቶፖች እና ታብሌቶች) በራስ የማገናኘት ቅንብር አላቸው። እነዚህ ቅንብሮች መሳሪያዎች በቀላሉ በቅርብ ካሉ አውታረመረቦች ጋር ግንኙነት ለመፍጠር እንዲችል ያደርገዋል። ይህ ከሚታመኑ አውታረመረቦች አንጻር ችግር የሌለው ሲሆን፣ ነገር ግን ደህንነታቸው አስተማማኝ ካልሆነ አውታረመረቦች ጋርም ግንኙነት እንዲኖር ሊያደርግ ይችላል። ይህንን ባህሪ በመሳሪያዎ ቅንብር ውስጥ ሊያጠፉት ይችላሉ። በተለይም ወዳልተለመዱ ስፍራዎች ጉዞ ሲያደርጉ እነዚህን ቅንብሮች ሁለጊዜም ያጥፉ። እንደተጨማሪ ጥንቃቄ፣ ህዝባዊ Wi-Fi ከተጠቀሙ በኋላ “forget network” የሚለውን መምረጥ ይችላሉ።

በተጨማሪም በህዝባዊ ስፍራዎች ላይ ሲሆኑ Bluetooth ዎንም መከታተል ያስፈልግዎታል። የ Bluetooth ግንኙነት ብዙ መሳሪዎች እርስ በርሳቸው ግንኙነት ለማድረግ እንዲችሉ ያደርጋል፣ በተጨማሪም ጠላፊ ክፍት የሆኑ Bluetooth ሞገዶችን በመፈልግ መሳሪያዎችን ሊቆጣጠር ይችላል። ይህንን ተግባር በስልክዎም ሆነ በሌሎች መሳሪዎችዎ ላይ በተለይም በማያውቁት ስፍራ ላይ ይዝጉት።

3. የፋይል መጋራትን ያጥፉት።

በህዝባዊ Wi-Fi ላይ ቢሚሆኑበት ጊዜ የፋይል መጋራት ምርጫዎችን ማጥፋትዎን እርግጠኛ ይሁኑ። በኦፐሬቲንግ ሲስተምዎ ላይ በመመስረት የፋይል መጋራትን ከ system preferences ወይም control panel ላይ መዝጋት ይችላሉ። AirDrop ማጥፋት የሚፈልጉት የፋይል መጋራት ምሳሌ አይነት ነው። አንዳንድ እንደ Windows/PC ያሉ ኦፐሬቲንግ ሲስተሞች የፋይል መጋራትን በራሳቸው የሚያጠፉ ሲሆን ይህም ለመጀመሪያ ጊዜ ከህዝባዊ አውታረመረብ ጋር ግንኙነት ሲያደርጉ "public" የሚለውን በመምረጥ ነው።

የፋይል መጋራትን የማጥፋት ቅደም ተከተሎች

PC ላይ:

1. ወደ Network and Sharing Center ይሂዱ።
2. ከዚያም advanced sharing settings የሚለውን ይቀይሩ።
3. የፋይል እና ፕሪንተር መጋራትን ያጥፉ።

ለ Macs:

1. ወደ System Preferences ይሂዱ።
2. Sharing የሚለውን ይምረጡ።
3. ሁሉንም ከምርጫ ውስጥ ያውጡ።
4. ከዚያም Finder ላይ AirDrop የሚለውን ጠቅ አድርገው Allow me to be discovered by: No One የሚለውን ይምረጡ።

ለ iOS AirDropን ከ Control Center ውስጥ አግኝተው ያጥፉት።

4. VPN ይጠቀሙ።

VPN (Virtual Private Network) በመሳሪያዎ ላይ መጫንን ከግምት ውስጥ ያስገቡ። VPN ለዲጂታል ግለኝነት በህዝባዊ Wi-Fi ከሁሉም በላይ ደህንነቱ አስተማማኝ የሆነው ነው። ውሂብዎ ከ እና ወደ መሳሪያዎ ሲተላለፍ እንዲመሰጠር የሚያደርግ ሲሆን እንደ መከላከያ "መስመር" አገልግሎት በመስጠት ውሂብዎ እንዳይታይ ያደርጋል።

5. ስለተመሰጠሩ ድረገጾች የ FBI ማስጠንቀቂያ – HTTPS።

የ FBI ማስጠንቀቂያ አድራሻቸው በ "https" ስለሚጀምር ድረገጾች ነው። የ "https" መገኘት እና የቁልፍ ምልክቱ የድሩ ተንቀሳቃሽ የተመሰጠረ እንደሆነ እና ጎብኚዎች ውሂቦችን ደህንነቱ አስተማማኝ በሆነ መንገድ መስራት ይቻልሉ ዘንድ ያደርጋል። ነገር ግን፣ የኢንተርኔት ወንጀለኞች ደህንነታቸው አስተማማኝ በሚመስሉ እና https ን በሚያካትቱ ድረገጾች ውስጥ ሰዎችን አጭበርብረው እንዲገቡ በማድረግ የህዘቡን አመኔታ ለራሳቸው ጥቅም ይጠቀሙበታል።

የ FBI ምክሮች:

- የኢሜይሉን ስም ብቻ አይመኑ ነገር ግን፡ አላማውን እና ይዘቱን ይመርምሩ።
- ከሚታወቅ አድራሻዎ ላይ ካለ ሰው የሚያጠራጥር ኢሜይል የሚደርስዎ ከሆነ መልእክቱ ትክክለኛ መሆኑን በመደወል ወይም ኢሜይል በመላክ ያረጋግጡ። ለሚያጠራጥር ኢሜይል ምላሽ አይስጡ።

- የፊደል ግድፈት ወይም ስህተት የሆነ ዶሜይን በሊንኩ ውስጥ (ምሳሌ፣ አንድ በ “.gov” ማለቅ ያለበት አድራሻ በ “.com” አልቆ ከሆነ) ያረጋግጡ።
- አንድ ድረገጽ የቁልፍ ምልክት ስላለው ወይም በ “https” ስለጀመረ ብቻ አይመኑት።

6. ጥንቃቄ የሚያስፈልገውን መረጃ መድረስ አይመከርም።

VPN ቢኖርዎትም እንኳን የግል ባንክ አካውንቶችን ወይም ተመሳሳይ እንደዚህ ያሉ የማህበራዊ ደህንነት ቁጥሮችን ደህንነታቸው አስተማማን ባልሆነ አውታረመረቦች ላይ መክፈት የለብዎትም። ህዝባዊ ደህንነታቸው አስተማማኝ የሆነ ግንኙነቶች እንኳ አንዳንድ ጊዜ ስጋት የሚያስከትሉ ናቸው። በህዝባዊ Wi-Fi ላይ የግድ እነዚህን መረጃዎች መክፈት ያለብዎ ከሆነ ሚዛናዊ የሆነ ምልከታ ከመወሰንዎ በፊት ያድርጉ። ለገንዘብ ልውውጥ፣ የስማርት ስልክዎን ሆትስፖት ተግባር እንደአማራጭ መጠቀሙ የተሻለ ነው።

7. ደህንነቱ አስተማማኘ የሆነ vs. ደህንነቱ አስተማማኝ ያልሆነ።

በጠቅላላው ሁለት አይነት ህዝባዊ Wi-Fi አውታረመረቦች አሉ: አስተማማኝ የሆነ እና ያልሆነ።

በሚችሉት ጊዜ ሁሉ ደህንነቱ አስተማማኝ የሆነነው ጥቅም ላይ ያውሉ። ደህንነቱ አስተማማኝ ያልሆነ ያለ ይለፍቃል ወይም ሎግኢን ለመግባት የሚቻልበት ነው። ደህንነቱ አስተማማኝ የሆነው ደግሞ ብዙ ጊዜ ተጠቃሚው ከደንቦች እና ሁኔታዎች ጋር እንዲስማማ፣ እንዲመዘገብ፣ ወይም ከመግባቱ በፊት የይለፍ ቃል እንዲያስገባ የሚያደርግ ነው።

8. የእሳት ግድግዳዎ እንዲበራ ያድርጉ።

ላፕቶፕ የሚጠቀሙ ከሆነ ህዝባዊ Wi-Fi ላይ ሲሆኑ የእሳት ግድግዳዎ እንዲበራ ያድርጉ። የእሳት ግድግዳ መሳሪያዎ ለጥቃቶች እንዳይጋለጥ የሚያደርግ ስራ የሚሰራ ነው። ተጠቃሚዎች የዊንዶውስ እሳት ግድግዳቸውን በ ብቅ ባዮች እና ማሳወቂያዎች ምክንያት ያጠፉት እና ከዚያም ሊረሱት ይችላሉ። PC ላይ መልሰው ሊያበሩት የሚፈልጉ ከሆነ ወደ Control Panel, "System and Security" ይሂዱ እና "Windows Firewall" የሚለውን ይምረጡ። የ Mac ተጠቃሚ ከሆነ ወደ "System Preferences" ይሂዱ እና "Security & Privacy" የሚለውን መርጠው "Firewall" ታብ ጋር በመሄድ ያብሩት።

9. አንቲቫይረስ ይጠቀሙ።

በተጨማሪም የቅርብ የሆነውን አንቲቫይረስ ሶፍትዌር ላፕቶፕዎ ላይ ይጫኑ። የአንቲቫይረስ ፕሮግራሞች ህዝባዊ Wi-Fi በሚጠቀሙበት ጊዜ ቫይረሶችን በመለየት ሲስተምዎ ውስጥ እንዳይገቡ ያደርጋል ማለት ነው። የሚታወቁ ቫይረሶች መሳሪያዎ ላይ ከገቡ ወይም ወይም አጠራጣሪ የሆነ ተግባር፣ ጥቃት ወይም ማልዌር ሲስተምዎ ውስጥ ከገባ የሚያሳውቅዎ ይሆናል።

10. ሁለት ወይም ከዚያ በላይ ደረጃ ያለውን ማረጋገጫ ይጠቀሙ።

ብዙ ደረጃ ያለውን ማረጋገጫ (MFA) በግል መረጃዎ ወደ ድረገጾች ሲገቡ ይጠቀሙ። ይህም ማለት ሁለተኛ ማረጋገጫ ኮድ አለዎ ማለት ሲሆን (ወደ ስልክዎ ቴክስት የሚደረግ ወይም ወደ መተግበሪያ የሚላክ ወይም አካላዊ ቁልፍ ነው) ይህም ተጨማሪ ጥበቃ ያደርግልዎታል። ስለዚህ አንድ ጠላፊ የተጠቃሚ ስም እና ይለፍ ቃልዎን ቢያገኝም እንኳን፣ ያለማረጋገጫ ኮድ አካውንትዎ ውስጥ መግባት አይችሉም ማለት ነው።

11. የግል መሳሪያዎችዎን ይከታተሉ።

ላፕቶፕዎን፣ ታብሌትዎን ወይም ስማርት ስልክዎን ህዝባዊ ስፍራዎች ላይ ወይም መኪና ውስጥ ጥለው አይሂዱ። የ Wi-Fi አውታረመረቦች ላይ ጥንቃቄ አድርገው ቢሆን እንኳ ሌላ ሰው መሳሪያዎን ከመውሰድ ወይም መረጃዎነት ከማየት አያግደውም። በዙሪያዎ ምን እንዳለ እና ምን አይነት ሰዎች እንዳሉ ክትትል ያድርጉ።

12. ሌሎች የኦንላይን ደህንነት ምክሮች።

ኦንላይን ሲሆኑ ደህንነትዎን ለማስተማመን የሚረዱ አንዳንድ ምክሮች የሚከተሉት ሲሆኑ በተለይም Wi-Fi ግንኙነቶችን የሚጠቀሙ ከሆነ ነው:

- ጠንካራ የይለፍ ቃሎችን ይጠቀሙ።
- መሳሪያዎን ይመስጠሩ።
- ከአጭበርባሪ ኢሜይሎች ይጠበቁ።
- ማህበራዊ ገጽ ላይ ምን እንደሚጥፉ ይጠንቀቁ። ከመጠን በላይ የሆኑ ዝርዝር መረጃዎች ጠላፊዎች የይለፍቃሎችን እንዲገምቱ ያደርጋሉ።
- የማያስፈልግዎትን መረጃ ያስወግዱ።
- አንድ አውታረመረብ ተጨማሪ ሶፍትዌር ወይም ተቀጥላ መጫን አለብዎ ካለ አይስማሙ።
- የቅርብ የሆኑ ፓቾች እና ሶፍትዌር እደሳዎች በመሳሪያዎችዎ ላይ መጫናቸውን በማረጋገጥ ራስዎን ይጠብቁ።