အင်တာနက်ဖြတ်တောက်ချိန်တွင် ဖိုင်ဝေမျှခြင်းနှင့် ဆက်သွယ်ခြင်း

ကက်ရှမီးယားဒေသမှာဆက်လက်ဖြစ်ပွားနေဆဲဖြစ်တဲ့ အင်တာနက် ဖြတ်တောက်ခြင်းနှင့် ဖြိုခွဲနှိမ်နင်းခြင်းသည် ဒီမိုကရေစီစနစ်တွင်းတွင်အကြာရှည်ဆုံးသောအင်တာနက်ဖြတ်တောက်မှုဖြစ်ပြီးဒေသတွင်းရှိ ပြည်သူများ၏အသက်ကို ပြင်းထန်ထိခိုက်သောသက်ရောက်မှု ဖြစ်စေခဲ့သည်။ ထိခိုက်ဒဏ်ရာပေါ်တွင် ရိုင်းပြစွာစော်ကားခြင်းဆင့်၍ ဒီဇင်ဘာ ၂၀၁၉တွင် WhatsApp၏ ရက် ၁၂၀ သုံးစွဲသူ မူဝါဒအရ ကက်ရှမီးယား၏ WhatsApp အကောင့်များသည် စတင်၍ ပိတ်သိမ်းခြင်းခံခဲ့ရသည်။

ယခုစာရေးသားသောအချိန်၊ဇန်နဝါရီ(၂၀၂၀)တွင်ကက်ရှမီးယားဒေသ၏အကန့်အသတ်မဲ့ အင်တာနက်ဖြတ်တောက်ခြင်းသည်တရားမဝင်သောအာဏာအလွဲသုံးစားမှုဖြစ်သည်ဟုအိန္ဒိယနိုင်ငံ၏ နိုင်ငံတော်တရားရုံးချုပ်တရားဝင်ဆုံးဖြတ်ခဲ့သည်။ ကန့်သတ်ထားသော မြန်နှုန်းမြင့်အင်တာနက် ဘရော့ဘင်နှင့် မိုဘိုင်းအင်တာနက်ကို အချို့နေရာများတွင် ပြန်လည်ရရှိသော်လည်း ခွင့်ပြုသောစာရင်း သန့်ရှင်းသောစာရင်း ဝက်ဘ်ဆိုက်များကိုသာရွေးချယ်ခွင့်ရှိသည်။အင်တာနက်ဖြတ်တောက်ခြင်းများသည်လူအများအားသတင်းအချက်အလက်မျှဝေခြင်းနှင့် ဆက်သွယ်ခြင်းအား ပိတ်ဆို့တားဆီးရန် ဒီဇိုင်းလုပ်ထားပြီး (လူများအား မိုဘိုင်းဖုန်းနှင့် SMS အချက်ပို့ခြင်း စသဖြင့် လုံခြုံမှုနည်းသော ဆက်သွယ်ရေးပုံစံစနစ်များကိုသာ သုံးရန် တွန်းပို့ခြင်းဖြင့်အာဏာပိုင်များအနေဖြင့်ကြားဖြတ်နားထောင်ခြင်းလေ့လာစောင့်ကြည့်ခြင်းများကို လွယ်ကူစေသည်) ။ကက်ရှမီးယားဒေသ၏ အတင်းကြပ်ဆုံးအင်တာနက်ဖြတ်တောက်ချိန်များ အတွင်းတွင် လူများစုသည် လက်ရေးစာများသုံးခြင်း စာပို့စာယူစနစ်များ သုံးခြင်းကိုသာ ယင်းတို့၏ချစ်ခင်သူများနှင့် သတင်းစကားပါးရန်အခြားရွေးချယ်စရာမရှိ၍ရွေးချယ်စရာအဖြစ်သတ်မှတ်ခဲ့ရသည်။ပိတ်ဆို့တားဆီးခြင်းအားလုံးကိုရှောင်တိမ်းနိုင်ရန် သေချာပေါက်နည်းလမ်း မရှိသေးသော်လည်း တက်ကြွလှုပ်ရှားသူနှင့် မိတ်ဆွေတို့၏ စကားလက်ဆုံများမှတဆင့် ကျွန်ုပ်တို့လေ့လာခဲ့သည်မှာ အချို့သော နည်းလမ်းများနှင့် ချဉ်းကပ်နည်းများသည် အော့ဖ်လိုင်းမျှဝေခြင်းနှင့် ဆက်သွယ်ခြင်းများ အခြေအနေပေါ်မူတည်ပြီး သင့်အတွက် အလုပ်ဖြစ်နိုင်မည်။ မှတ်ချက်ပြုရန်မှာ အချို့ရွေးချယ်နိုင်သောလမ်းများသည် စတင်ပြင်ဆင် setup လုပ်ရန်အတွက် အင်တာနက်လိုအပ်သည်။ (app ဒေါင်းလုပ်လုပ်ခြင်း စသဖြင့်)

အနီးကပ်ဆက်သွယ်မှုစနစ် NFC, Bluetooth ကြိုးမဲ့အနီးကပ်ဆက်သွယ် Wifi Direct မှတဆင့် ဖိုင်မျှဝေခြင်း

သင်ဖုန်းနဲ့ နီးရာတွင်ရှိသော ဖုန်းသို့မဟုတ်device တခုကိုဆက်သွယ်ရန် အင်တာနက်ဆက်သွယ်မှုရှိရန် မလိုအပ်ပါ။Bluetooth,Wifi,Direct,NearFieldCommunicationNFC/နီးစပ်ရာကွင်းပြင်ဆက်သွယ်စနစ်အင်တာနက်မလိုအပ်ပါ။(တခါတရံ အင်ဒရိုက်ဘိန်းဟုလည်းခေါ်သည်)။Bluetooth နှင့် Wifi Direct နှစ်ခုစလုံးသည် ကြိုးမဲ့ဆက်သွယ်နည်းပညာ ဖြစ်ပြီ ဖုန်းသို့မဟုတ်deviceနှစ်ခုကို ချိတ်ဆက်ပွိုင့် သို့မဟုတ် ကွန်ယက်ဖြန့်ချီစက်မရှိဘဲ "စုံတွဲဆက်သွယ်" နိုင်ပါသည်။ Wifi Directက ပိုမိုကျယ်ဝန်းသော အကွာအဝေးကို Bluetooth ထက်ပို၍လျင်မြန်သောဒေတာလွှဲပြောင်းမှုပံ့ပိုးနိုင်ပါသည်၊သို့သော်ပါဝါကိုအလွန်တရာပိုသုံးသည်။ တချိန်တည်းမှာ NFC သည် ပိုမိုတိုတောင်းသော အကွာအဝေးကို Bluetooth or Wifi Direct ထက်နှေးသော လွှဲပြောင်းနှုန်းဖြင့် သို့သော် ပိုမိုမြန်ဆန်စွာချိတ်ဆက်ပြီး ပါဝါသုံးနှုန်းနည်းသည်။ ထို့ကြောင့် ပမဏနည်း လွှဲပြောင်းခြင်းဖြစ်မယ် စက်နှစ်ခုလုံးလက်ထဲရှိမယ်ဆို အသုံးဝင်သည်။

Wifi Directကတော့ဘလူးတုထက်စာရင်ဝေးဝေးရောက်ပြီး ဒေတာတွေကို မြန်မြန်ပြောင်းရွှေ့နိုင်စွမ်းရှိပေမယ့် ပါဝါသုံးတာအရမ်းများပါသည်တချိန်တည်းမှာNFCအနီးကပ်ဆက်သွယ်မှုလေးစင်တီမီတာပိုပြီးနီးနီးအကွာအဝေးနဲ့ ပြောင်းရွှေ့ချိန်လည်းပိုနှေးကွေးပါသည်သို့သော် သူက ဆက်သွယ်မှုပိုမြန်ပြီး ပါဝါသုံးတာပိုနည်းတာမို့ ခပ်မြန်မြန်နဲ့ နည်းနည်းပဲ ပြောင်းရွှေ့မယ် စက်နှစ်ခုလုံးလက်ထဲမှာရှိမယ်ဆို အသုံးဝင်ပါတယ်။
သင့်ရဲ့ဖုန်းမှာBluetooth, Wifi Direct or NFC features အင်္ဂါရပ်များက တပါတည်းပါလာပြီး မျှဝေဖို့နည်းလမ်းများကိုလည်း ပြသထားနိုင်ချေရှိပါသည်။ ဒါ့အပြင် ဖိုင်းတွေကိုမျှဝေတဲ့ အင်္ဂါရပ်မျိုးဖြစ်တဲ့ [Files by Google](#) app ကဲ့သို့နည်းပညာများလည်း ပေါင်းစပ်ထားမှာပါ။

အရေးကြီးမှတ်ချက်။ဒီဝန်ဆောင်မှုတွေကတော့ ဆက်သွယ်ဖို့လွယ်ကူပြီး အားနည်းချက်ကတော့ လုံခြုံမှုမရှိပါ။ Bluetooth and wifi များသည် တည်နေရာဒေသကို ခြေရာခံခြင်း သင့်ဖုန်းdeviceအချက်အလက်တွေကို စုံစမ်းစစ်ဆေးလို့ရနိုင်ပါသည်။ ကြားဖြတ်ဖောက်ထွင်းသူများကလည်း သင့်ဖုန်းdevice ကို စုံတွဲဆက်သွယ်ဖို့ ကြိုးပမ်းတာမျိုး မလိုချင်တဲ့ဖိုင်တွေကို ပို့လိုက်တာမျိုး သို့မဟုတ် ထိခိုက်လွယ်တဲ့အခြေအနေမှာ သင့်ဖုန်းdeviceကို ထိန်းချုပ်တာမျိုးတွေ လုပ်နိုင်ပါသည်။**ပိုပြီးလုံခြုံမှုရှိဖို့ဆိုရင် စက်တွေကို မသုံးတဲ့အချိန်မှာ ဝန်ဆောင်မှုတွေအားလုံးကိုပိတ်ထားပြီး လုံခြုံသောနေရာမှ ပြန်ဖွင့်တာမျိုး app တွေကို လိုအပ်တာဘဲ ဘာလဲ/ဘယ်သူလဲခွင့်ပြုချက် ကန့်သတ်ထားတာမျိုး ဖုန်းလုံခြုံရေးစနစ် ကိုလေ့ကျင့်ပြီး update အမြဲလုပ်နေတာမျိုး ခိုင်မာသောလျှို့ဝှက်နံပါတ် passcode ထားတာမျိုးလုပ်ရမှာဖြစ်သည်။**

ကြိုးမဲ့စနစ်ဖြင့်ဖိုင်များကိုမျှဝေခြင်း ကြိုးမဲ့ဆက်သွယ်မှုဧရိယာကွန်ယက်

ကြိုးမဲ့hard drive သို့မဟုတ် flash drive များကို အဖွဲ့တွင်း သို့မဟုတ် လူများစုကို တပြိုင်နက်တည်း ဖိုင်မျှဝေရာတွင် သုံးနိုင်သည်။Wifi driveသည်များသောအားဖြင့် ညွှန်ကြားချက်များနှင့်အတူ သို့မဟုတ် drive ဆက်သွယ်ရန် app များပါပြီး သုံးစွဲရန် လွယ်ကူသည်။ လုံခြုံရေးအတွက် drive ကို လျှို့ဝှက်နံပါတ်လုပ်ရန် သတိရပါစေ။ကြိုးမဲ့driveမရှိဘူးဆိုရင်ပုံမှန်USBdriveကိုကြိုးမဲ့ကွန်ယက်ဖြန့်ချီကိရိယာမှာပလပ်ထိုးပြီးသုံးလို့ရပါ သည်။USBအပေါက်ပါသောခရီးသွားကွန်ယက်ဖြန့်ချီကိရိယာသည်စျေးသက်သာပြီးသယ်ယူရန်လွယ်ကူသည်။သုံး စွဲသူသည်USBdriveကိုအင်တာနက်မလိုဘဲဒေသတွင်းဧရိယာကွန်ယက်မှတဆင့်ဆက်သွယ်နိုင်သည်။
ဖုန်းထဲမှာရှိသောဖိုင်များကို USB drive နှင့် ဝင်ရောက်ချိတ်ဆက်ရန် ဖိုင်မန်နေဂျာ app ကို သုံးစွဲပြီး[Solid Explorer](#) ကဲ့သို့ကွန်ယက်တွင်းရှိ သိုလှောင်ခန်းများကို ဆက်သွယ်နိုင်သည်။ ကွန်ယက်ဖြန့်ချီကိရိယာ၏ အိုင်ပီလိပ်စာကို သင့်ဖုန်း၏ advanced wifi settings တွင် တွေ့ရှိနိုင်သည်။
နောက်တခုသုံးနိုင်တဲ့ နည်းလမ်းတခုက [PirateBox](#) လို့ခေါ်တဲ့ ကိုယ်တိုင်လုပ် ပရောဂျက်ဖြစ်ပြီးတော့ လိုင်စင်ရှိဖရီးဆော့ဖ်ဝဲဖြစ်သည်။အပေါ်မှာပြထားသလိုပဲဖိုင်တွေကိုမျှဝေနိုင်ပြီးPirateBoxကအမည်မသိမျှဝေခွ င့်ပေးမှာဖြစ်တဲ့အပြင်ချက်နဲ့ မတ်ဆေ့ပို့နိုင်တဲ့ အင်္ဂါရပ်များလည်းပါဝင်ပါသည်။ PirateBox ကိုပြင်ဆင်ခြင်း setupလုပ်ဖို့အတွက် ဆော့ဖ်ဝဲ အပိုင်းအစအနည်းငယ်ကို download, install နဲ့ setup လုပ်ရမှာဖြစ်ပါသည်။ [ညွှန်ကြားချက်များ](#)ကို Pirate Box ဝက်ဘ်ဆိုက်တွင် ကြည့်ပါ။

မိတ်ဆွေချင်းချက်လုပ်ပြီးဆက်သွယ်ခြင်း

တက်ကြွလှုပ်ရှားသူကွန်ယက်များမှတစ်ဆင့်သတိပြုမိလာတဲ့အသစ်ကဲ့သို့ မိတ်ဆွေချင်းအချက်ပို့ဆက်သွယ်တဲ့ app များတွင် Briar and Bridgefy တို့ဖြစ်သည်။ကျွန်ုပ်တို့ သုံးစွဲဖူးခြင်းမရှိသေးသော်လည်း စမ်းသပ်သုံးစွဲဖူးသူများကို သိရှိပါသည်။

Briar သည် ပွင့်လင်းအရင်းအမြစ်ဖြစ်ပြီး နှစ်ဖက်လုံးလျှို့ဝှက်ထိန်းသိမ်း သောစနစ်ဖြင့် အချက်ပို့သောapp ဖြစ်ပြီးဗဟိုဆာဗာကို အားကိုးခြင်းမရှိဘဲသုံးစွဲသူများ၏ဖုန်း(device)များကိုsyncsဆွဲယူခြင်း(သုံးစွဲသူတိုင်း၏ device တွင် အကြောင်းအရာများကို အသက်ဝင်နေမည်။အင်တာနက်မသုံးဘဲ Bluetooth or Wifi သုံးရုံဖြင့်လည်း ဆွဲယူနိုင်သည်။ (အင်တာနက်ရချိန်တွင် Tor ကွန်ယက်ကိုသုံးပြီး ဆွဲယူနိုင်သည်) Briar သည် ကိုယ်ပိုင်အုပ်စုဖွဲ့ခြင်း အများသုံးဖိုရပ်များ ဘလော့ဂ်များလည်း တည်ဆောက်နိုင်သော အင်္ဂါရပ်များပါသည်။ အော့ဖ်လိုင်းသုံးချိန်တွင် သင်၏အကွာအဝေးသည် Bluetooth or Wifi အကွာအဝေးကဲ့သို ကန့်သတ်ချက်ရှိသည်။ (အများဆုံး တရာမီတာ)
တချိန်တည်းတွင်Bridgefyသည်နှစ်ဖက်လုံးလျှို့ဝှက်လုံခြုံသော(တိုက်ရိုက်အသံလွှင့်သောအင်္ဂါရပ်သုံးခြင်းမှအပ) အချက်ပို့သော app ဖြစ်ပြီး Bluetooth ကိုသုံးပြီး အချက်ပို့သည်။ Brairနဲ့မတူသောအချက်က မတ်ဆေ့သည်အကွာအဝေးရှည်ရှည်ခရီးရောက်နိုင်သည်။အခြားBridefyသုံးစွဲသူများ၏ပိုက်စိတ်တိုက်ထားသောကွန်ယက်မှ ခုန်ဆွခြင်း (ရည်ရွယ်ပြီးပို့သူသာဖတ်လို့ရမည်ဖြစ်သည်)။ Bridgefy သည် Briar ကဲ့သို့ ကိုယ်ပိုင်အဖွဲ့၊ဖိုရမ်၊ဘလော့ဂ်အင်္ဂါရပ်များမပါရှိသော်လည်းတိုက်ရိုက်လွှင့်သောစွမ်းရည်ရှိပြီးတပြိုင်တည်းတွင် သင့်ဆက်သွယ်သူ စာရင်းထဲတွင် မပါသော Bridgefy သုံးစွဲသူ ၇ ယောက်ဆီအထိ ပို့နိုင်သည်။ (လိုအပ်ချက်အရ တိုက်ရိုက်လွှင့်သော မတ်ဆေ့များသည် လျှို့ဝှက်ထိန်းသိမ်းခြင်း encrypted မဖြစ်ပါ)။

လျှို့ဝှက်ထိန်းသိမ်းSMSမှတဆင့်ဆက်သွယ်ခြင်း

ဖုန်းလိုင်းနဲ့သွားသော အချက်ပို့ခြင်းသည် အက်စ်အမ်အစ်ပို့ခြင်းသည် အင်တာနက်အပေါ်မှီကပ်စရာမလိုပါ၊ အင်တာနက်ဖြတ်တောက်ထားခြင်းတွင်လည်း အသုံးပြုနိုင်သည်။ သို့သော် လုံခြုံမှုလုံးဝမရှိပါ။ အင်တာနက်ရှိမှ သုံးလို့ရသော app များဖြစ်သည့် WhatsApp or Signal နဲ့မတူသည်မှာ SMS သည် နှစ်ဖက်စလုံးကို လျှို့ဝှက်ထိန်းသိမ်းထားခြင်းမရှိဆိုလိုသည်မှာ အချက်ပို့ခြင်းနှင့် သူတို့၏ metadataများသည် အစိုးရနည်းတူ ဖုန်းဝန်ဆောင်မှုပေးသူများဟတ်ကာများကကြားဖြတ်၍ထိုအချက်ပို့ခြင်းများကိုဖတ်ရှုနိုင်သည်။
SMSများသည်လှည့်စားနိုင်သည်။ဆိုလိုသည်မှာပို့ပေးသူသည်သူတို့၏လိပ်စာအချက်အလက်ကိုလိမ်လည်ပြီးတခြားသူအနေနဲ့ အယောင်ဆောင်ပြီးပေးပို့နိုင်သည်။
SMS ပို့စရာရှိလျှင် Silence ဆိုတဲ့ app သည် နှစ်ဖက်စလုံးကို လျှို့ဝှက်ထိန်းသိမ်းထားသော SMS ဖြစ်သည်။ ပွင့်လင်းအရင်းအမြစ်ဖြစ်ပြီးSignal၏လျှို့ဝှက်ထိန်းသိမ်းခြင်းလုပ်ထုံးလုပ်နည်းကိုသုံးထားသည်။ကျွန်ုပ်တို့ကိုယ်တိုင်စမ်းသပ်ဖူးခြင်းမရှိသော်လည်းအခြားသူများသုံးသည်ကိုကြားဖူးသည်။ပေးပို့သူရောလက်ခံသူပါinstallလုပ်ထားရမှာဖြစ်ပြီးလဲလှယ်သောသော့ချက်ရှိရမှာဖြစ်သည်။SMSသည်သင့်ရဲ့တယ်လီကွန်းဆာဗာကိုဖြတ်ပြီးမှသွားမှာဖြစ်တဲ့အတွက်Silenceကိုသုံးရင်တောင်မှလျှို့ဝှက်သောမတ်ဆေ့ကိုပို့မှာဖြစ်သော်လည်း မတ်ဆေ့ရဲ့metadata တွေကိုတော့ တယ်လီကွန်း ကုမ္ပဏီတွေကနေ အချက်အလက်ရှာဖွေနိုင်မှာ ဖြစ်ပါသည်။

တစ်စိတ်တစ်ပိုင်းဖြတ်တောက်ခြင်းပိတ်ပင်တားဆီးထားသောဆိုက်ဒ်များကိုရှောင်တိမ်းခြင်း

မကြာခဏအားဖြင့် အင်တာနက်ဖြတ်တောက်ခြင်းသည် အင်တာနက်တစ်ခုလုံး ပြတ်အောင်ပိတ်ခြင်းမဟုတ်ဘဲ အချို့သီးခြားဝက်ဘ်ဆိုက်ဒ်နှင့်ဆိုရှယ်မီဒီယာများကိုသာပိတ်ပင်ခြင်းလည်းဖြစ်နိုင်သည်။အာဏာပိုင်အစိုးရသည် အင်တာနက်ဝန်ဆောင်မှုပေးသူISPများမှတစ်ဆင့်အိုင်ပီလိပ်စာပေါ်အခြေခံသောပိတ်ပင်ခြင်း အကြောင်းအရာသို့မဟုတ် DNS looups ဒိုမိန်းအမည်စနစ်ရှာဖွေခြင်းစနစ်ကတစ်ဆင့် ပိတ်ပင်နိုင်သည်။ ဆိုက်ဒ်တခုကပိတ်ပင်ထားခြင်းခံရသလားဆိုတာမသေချာဘူးလားအဖွဲ့အစည်းများဖြစ်သော Open Observatory of Network Interference and Netblocks စသောအဖွဲ့အစည်းများက လေ့လာစောင့်ကြည့်ချင်း အင်တာနက်ပြတ်တောက်မှုနဲ့ ပတ်သက်ပြီး တိုင်းတာခြင်း ဆင်ဆာဖြတ်ခြင်းကို ကမ္ဘာနှင့်တဝန်းတွင်လုပ်ဆောင်သည်။ကံကောင်းထောက်မသည်မှာသင့်တွင်အင်တာနက်ဝင်ရောက်ချိတ်ဆက်ခွင့် ရှိသမျှ ကာလပတ်လုံး တစ်စိတ်တစ်ပိုင်းပိတ်ဆို့ခြင်းကို ကျော်ဖြတ်နိုင်သော နည်းလမ်းများရှိသေးသည်။ လျှို့ဝှက်ထိန်းသိမ်းခြင်းencryptionနှင့်အတူပိတ်ဆို့ထားသောဆိုက်ဒ်များကိုရှောင်တိမ်းပြီးအသုံးပြုခြင်းသည်လည် း သင့်နိုင်ငံတွင် ရာဇဝတ်ပြစ်မှုအဖြစ်သတ်မှတ်နိုင်ကြောင်း သတိပြုပါ။

ဗီပီအန် ခေါ် လျှို့ဝှက်ဆက်သွယ်ကွန်ယက်

အိုင်ပီအခြေခံနှင့်အကြောင်းအရာကိုအခြေခံသောပိတ်ပင်တားဆီးခြင်းကိုရှောင်ကွင်းကျော်ဖြတ်ရန်နည်းလမ်းတခု မှာProtonVPNorTunnelBearကဲ့သို့လျှို့ဝှက်ကွန်ယက်စနစ်ဗီပီအန်သုံးခြင်းဖြစ်သည်။ ဗီပီအန်မှတစ်ဆင့်ဆက်သွယ်သောအခါအင်တာနက်အသွားအလာလမ်းကြောင်းသည်လျှို့ဝှက်လုံခြုံပြီးဗီပီအန်ဆာ ဗာမှတစ်ဆင့်တစ်ခြားအရပ်ဒေသ၊အခြားနိုင်ငံအစရှိသဖြင့်ပြောင်းသွားပြီးအမှန်တကယ်ရည်ရွယ်ရာအရပ်နှင့်သင့် အင်တာနက်အသွားအလာလမ်းကြောင်းအကြောင်းအရာကိုသင့်အင်တာနက်ဝန်ဆောင်မှုပေးသူအား ဖုံးကွယ်သည်။ ဖြတ်သန်းသွားသောကြောင့်တကယ်နေရာအစစ်အမှန်နဲ့ပါဝင်မှုများကိုလမ်းကြောင်းပြောင်းပေးသည်။ တချို့နိုင်ငံအစိုးရများက ဗီပီအန်သုံးစွဲမှုကို ပိတ်ပင်ခြင်း သို့မဟုတ် ပိတ်ထားသော ဗီပီအန်မှ တဆင့်သုံးစွဲမှုကို ခြေရာခံခြင်းများ လုပ်နိုင်သည်။ အရေးကြီးသည်မှာစိတ်ချရသော ဗီပီအန်ကိုသုံးစွဲခြင်း အချက်အလက်များကို မစုဆောင်းသောတစ်ခုကိုသုံးစွဲခြင်းကိုပြုသင့်သည်။မည်သည့်နိုင်ငံတွင်ဗီပီအန်ကရှိနေသလဲသူတို့ရဲ့ ဆုံးဖြတ်သုံးသပ်မှုများသည်တရားဆိုင်ရာလမ်းကြောင်းများရှိမရှိတစ်ချို့အစိုးရသည်ဗီပီအန်ကိုခွင့်ပြုသော်လည်း သင့်အချက်အလက်များကို စုံစမ်းထောက်လှမ်းခြင်း လေ့လာစစ်ဆေးခြင်းများလုပ်ဆောင်သည်။

DNS ဆာဗာ ဒိုမိန်းအမည်စနစ်

DNS (ဒိုမိန်းအမည်စနစ်) ဆာဗာတွေဟာ ဒိုမိန်းအမည်တွေကို ဘာသာပြန်ပြီး အလုပ်လုပ်တဲ့ သို့မဟုတ် သုံးစွဲသူအနေနဲ့ နံပါတ်ပါသော အိုင်ပီလိပ်စာများကို ရိုက်ထည့်ပြီး အင်တာနက် ဝက်ဘ်စာမျက်နှာတွေကို ခွဲခြားသတ်မှတ်တဲ့ URL တွေ ဖြစ်ပါသည်။ ISP အင်တာနက်ဝန်ဆောင်မှုပေးသူသည် ဒိုမိန်းအမည်စနစ် DNS ဆာဗာများကို ပြုပြင်ပြီး အချို့မေးမြန်းချက်များကို ထိန်းချုပ်ခြင်း ဝက်ဘ်ဆိုက်ဒ်မရှိပါ ဟူ၍ မမှန်သောစာမျက်နှာများကိုပြန်ပို့ခြင်းလုပ်သည်။
၂၀၁၄ ခုနှစ် တူရီကီရွေးကောက်ပွဲကာလာအတွင်း တူရကီဝန်ကြီးချုပ် Recep Tayyip Erdogan က တွစ်တာကို ပိတ်ရန်ကြိုးစားတုန်းက ထိုနည်းကိုသုံးခဲ့သော်လည်း ပိတ်ပင်ခြင်းကို တက်ကြွလှုပ်ရှားသူများက လျင်မြန်စွာဖောက်ထွင်းပြီးဗီပီအင်သုံးရန်နှင့်ဒိုမိန်းအမည်စနစ်DNSဆာဗာပြောင်းရန်အသုံးဝင်သည့်အချက်များကို တဆင့်ပြီးတဆင့် တဆင့်ချင်း တားဆီးနိုင်နိုင်ခဲ့သည်။

မူလDNSဆာဗာကို ဖုန်းရဲ့network သို့မဟုတ် wifi setting မှာ ပြောင်းလို့ရပါသည်။ ဆာဗာသုံးတဲ့အခါ မူလDNSဆာဗာ တမျိုးတည်းမသုံးဘဲ အပြောင်းအလဲဆာဗာတွေဖြစ်တဲ့ Google Public DNS or quad9 တွေကို ပြောင်းလဲသုံးခြင်းဖြင့် DNSကို အခြေခံပြီး ပိတ်ဆို့တာတွေကို လှည့်ပတ်သွားနိုင်မှာဖြစ်ပါသည်။ Quad 9 တွင်Quad 9 Connect . ဟုခေါ်သော app တစ်ခုလည်းရှိသည်။ယခုစာရေးနေသည့်အချိန်တွင် Quad9 connect appသည် စတင်အသုံးပြုနိုင်ရန် စမ်းသပ်သည့်အဆင့်မှာသာရှိသေးသည်။

ပိတ်ပင်ခြင်းကိုရှောင်တိမ်းနိုင်သောအသုံးများသည့်နည်းလမ်းနှစ်မျိုးသာရှိသည်။
အတွင်းကျကျအချက်အလက်များကိုလေ့လာလိုလျှင်“InternetSociety, AccessNow, Security-in-a-Box and EFF” တွင် အတွင်းကျကျ အချက်အလက်များကိုရရှိနိုင်ပါသည်။