EFF'S SURVEILLANCE SELF-DEFENSE

ကိုယ့်အတွက် အသင့်တော်ဆုံး VPN ကိုရွေးချယ်ခြင်း

https://ssd.eff.org/en/about-surveillance-self-defense

LOCALIZATION LAB

ကိုယ့်အတွက် အသင့်တော်ဆုံး VPN ကိုရွေးချယ်ခြင်း

နောက်ဆုံးစိစစ်ထားသည့်ရက်စွဲ - ၂၀၂၁ ခုနှစ် ဇွန်လ ၂၅ ရက်

VPN ရဲ့ အရှည်က Virtual Private Network ဖြစ်ပါတယ်။ VPN ချိတ်ဆက်အသုံးပြုရင် ကိုယ်ပေးပို့တဲ့ အချက် အလက် အားလုံးဟာ (ဥပမာ ဝက်ဘ်ဆိုဒ်သုံးရင် ဆာဗာတွေထံ ဝင်ခွင့်တောင်းရတာမျိုး) ကိုယ့် ISP ဆီက မဟုတ်ဘဲ VPN ဆီကနေလာတဲ့ ပုံပေါ်အောင် လုပ်ပေးပါတယ်။ ဒီလိုလုပ်ခြင်းဖြင့် ကိုယ်ရေးကိုယ်တာ လျှို့ဝှက် မှုအတွက် အရေးကြီးအရာတစ်ခုဖြစ်တဲ့ ကိုယ့် IP လိပ်စာ ကို ဖုံးထားပေးနိုင်ပါတယ်။ IP လိပ်စာဟာ ကိုယ်ဘယ်နေမှာ ရှိနေသလဲဆိုတာကို ယေဘူယျဖော်ပြနိုင်တာကြောင့် မိမိဘယ်သူဘယ်ဝါဆိုတာ သိသာပေါ်လွင်စေနိုင်တဲ့ အရာတစ်ခု ဖြစ်ပါတယ်။

လက်တွေ့ VPN အသုံးပြုခြင်း

- ကိုယ်ရဲ့အင်တာနက်ပေါ်က လုပ်ဆောင်ချက်တွေကို စူးစမ်းသူတွေမသိရှိအောင် ကာကွယ်ပေးနိုင်ပါတယ်။ အထူးသဖြင့် ကော်ဖီဆိုင်၊ လေဆိပ်၊ စာကြည့်တိုက် စတဲ့အများပြည်သူသုံး နေရာတွေက မလုံခြုံတဲ့ Wi-Fi ကွန်ယက်တွေနဲ့ ချိတ်ဆက်ပြီး အင်တာနက်သုံးမယ်ဆိုရင် VPN ကိုပိုအသုံးပြုသင့်ပါ တယ်။
- ကွန်ယက်ပေါ်မှာ အချို့သော ဝက်ဘ်ဆိုဒ်တွေ၊ ဝန်ဆောင်မှုတွေ အသုံးမပြုနိုင်အောင် ပိတ်ဆို့ထား တာရှိရင် ရှောင်ရှားနိုင်ပါတယ်။ ဥပမာ ကိုယ်က ကျောင်းကွန်ယက်ကနေ အင်တာနက်သုံးနေတာမျိုး၊ တားဆီးပိတ်ပင်မှုများတဲ့ နိုင်ငံတစ်ခုမှာ အင်တာနက်သုံးပြီး အလုပ်လုပ်တာမျိုးဆို အသုံးဝင်ပါတယ်။ နိုင်ငံအလိုက် VPN အသုံးပြုမှုနဲ့ ပတ်သက်တဲ့ မူဝါဒကွဲနိုင်တာကြောင့် ဘယ်လိုကန့်သတ်ပိတ်ပင်မှုတွေ ရှိတယ်ဆိုတာ သတိပြုပါ။
- ကုမ္ပဏီတွင်းကွန်ယက် intranet နဲ့ ဘယ်နေရာကနေမဆို ချိတ်ဆက်နိုင်စေပါတယ်။ နိုင်ငံခြားခရီး သွားနေချိန်ဘဲဖြစ်ဖြစ်၊ အိမ်မှာနေရင်းဘဲဖြစ်ဖြစ်၊ ရုံးမတက်နိုင်တဲ့ အခြားအချိန်မှာဘဲဖြစ်ဖြစ် ရုံးရဲ့ intranet ကိုဝင်ပြီး အသုံးပြုနိုင်စေပါတယ်။

လူအများ အမှတ်မှားတတ်တဲ့ကိစ္စတစ်ခုက VPN တွေကို ကွန်ပျူတာတွေပေါ်မှာသာ သုံးသင့်တယ်လို့ ထင်ကြ တာဖြစ်ပါတယ်။ ဖုန်းကနေတစ်ဆင့်လည်း ကိုယ်မသိတဲ့ Wi-Fi ကွန်ယက်တွေနဲ့ လှမ်းချိတ်မယ်ဆိုရင် ကွန်ပျူတာ ကချိတ်သလိုဘဲ အန္တရာယ်ရှိနိုင်ပါတယ်။ ဒါကြောင့် ဖုန်းကုမ္ပဏီနဲ့ အင်တာနက်ဝန်ဆောင်မှုပေးသူ (ISP) တို့ အကြား သတင်းအချက်အလက်အသွားအလာတွေကို ကုဒ်ဖြင့်ပြောင်းလဲ နိုင်အောင် ဖုန်းမှာလည်း VPN သုံးသင့်ပါတယ်။

VPN နဲ့ ပတ်သက်လာရင် အားလုံးအဆင်ပြေစေမယ့် နည်းလမ်းတစ်ခုရယ်လို့ မရှိပါဘူး။ အီးမေးလ်ဝန်ဆောင်မှု လိုဘဲ VPN ဝန်ဆောင်မှုတွေလည်း မြောက်များစွာရှိတဲ့အတွက် ကိုယ့်အတွက် အသုံးအဝင်ဆုံးဖြစ်မယ့် ဝန်ဆောင်မှုကို ရွေးချယ်ပါ။ ကိုယ်မယုံကြည်တဲ့ ကွန်ယက်တွေနဲ့ ချိတ်ဆက်ဖို့လုပ်တဲ့အခါ ကိုယ်ရွေးချယ်တဲ့ VPN ဝန်ဆောင်မှုအပေါ်မူတည်ပြီး ပိုမိုလုံခြုံမှုရှိနိုင်ပါတယ်။ ဒါပေမယ့် အသုံးပြုတဲ့ VPN ကတော့ ယုံကြည်ရဖို့ လိုပါတယ်။

ဒါဆို ကိုယ့်မှာ VPN သုံးဖို့လိုသလား။ ဘယ်လို VPN ကိုရွေးချယ်အသုံးပြုသင့်သလဲ။ ဒီလိုမေးခွန်းတွေကို ဖြေဖို့ အတွက် စဉ်းစားစရာကိစ္စတွေအများကြီးရှိပါတယ်။ ဒီလမ်းညွှန်မှာတော့ ဘယ်ဝန်ဆောင်မှုက မိမိအတွက် အသုံး အဝင်ဆုံးဖြစ်မယ်ဆိုတာ စဉ်းစားလို့ရအောင်ကူညီပေးပြီး VPN ရွေးချယ်တဲ့အခါ ဘယ်လိုအကြောင်းအရင်းတွေ ပေါ်မူတည်ပြီး ဆုံးဖြတ်သင့်သလဲဆိုတာ ညွှန်ပြပေးပါမယ်။

ဒါဆို အခြေခံနဲ့ စလိုက်ရအောင် - VPN တွေက ဘာလုပ်ပေးတာလဲ။

ဒီမိုကရေစီနှင့် နည်းပညာဆိုင်ရာ စင်တာ (Center for Democracy & Technology) မှထုတ်ပြန်ထားတဲ့ ဤရှုင်းလင်းချက် မှာ VPN ကိုဒီလိုအဓိပ္ပါယ်ဖွင့်ဆိုထားပါတယ်။ “မိမိရဲ့ အင်တာနက်အသုံးပြုလုပ်ဆောင်မှု များကို အပြင်လူတွေ စောင့်ကြည့်ခြင်း၊ ကြားဖြတ်ပြောင်းလဲခြင်းများ မပြုလုပ်နိုင်စေရန် အင်တာနက်ပေါ်မှ လုပ်ဆောင်ချက်အသွားအပြန်ကိစ္စများကို လျှို့ဝှက်ခေါင်းသဖွယ်ဖန်တီးပြီးကာကွယ်ပေးပါတယ်။ ဒီလျှို့ဝှက်ခေါင်း ထဲက အသွားအပြန်လုပ်ဆောင်ချက်များကို ကုဒ်ဖြင့်ပြောင်းလဲပြီး VPN ထံသို့ ပို့ပေးပါတယ်။ ဒါ့ကြောင့် ကြားခံအဖွဲ့တွေဖြစ်တဲ့ အင်တာနက်ဝန်ဆောင်မှုပေးသူ (ISPs) တွေ၊ အများသုံး Wi-Fi ကို စောင့်ကြည့်နေတဲ့ ဟတ်ကာတွေဟာ VPN အသုံးပြုသူရဲ့ အင်တာနက်လုပ်ဆောင်ချက်များကို စောင့်ကြည့်ခြင်း၊ ကြားခံလူ တိုက်ခိုက်မှုများလုပ်ခြင်းတို့ ပြုလုပ်ဖို့ ခက်ခဲမှာဖြစ်ပါတယ်။ VPN ဆီကနေမှတစ်ဆင့် လိုချင်တဲ့နေရာကို အချက်အလက်တွေက ဆက်သွားတဲ့အတွက် အသုံးပြုသူရဲ့ နဂို IP လိပ်စာ ကို ခြေရာခံဖို့ ခက်ခဲစေပါတယ်။ ဒါကြောင့် ပေးပို့တဲ့အချက်အလက်တွေကတစ်ဆင့် အသုံးပြုသူရဲ့ တည်နေရာကို ခြေရာခံဖို့ ကြိုးပမ်းရင် VPN ကြားခံထားတာကြောင့် မြင်ရမှာမဟုတ်ပါဘူး။”

ရှေ့ဆက်ပြီး VPN တွေ ဘာလုပ်သလဲဆိုတာကို ဆက်မဖတ်ခင် ဒီမိုကရေစီနှင့် နည်းပညာဆိုင်ရာ စင်တာ (Center for Democracy & Technology) ကထုတ်ပြန်ထားတဲ့ ဆောင်းပါးတစ်ပုဒ်ကို အစအဆုံးဖတ်ကြည့်ဖို့ အကြံပြုလိုပါတယ်။

စဉ်းစားရန် အချက်များ - VPN တွေက ဘာမလုပ်နိုင်ဘူးလဲ

အင်တာနက်ပေါ်က မိမိရဲ့သတင်းအချက်အလက် အသွားအလာကို အများသုံးကွန်ယက်တွေပေါ်မှာ စောင့်ကြည့် စုံစမ်းလို့မရအောင် VPN ကကာကွယ်ပေးနိုင်ပေမယ့်လည်း ပုဂ္ဂလိကကွန်ယက်ကို အသုံးပြုနေရင်တော့ အချက် အလက်တွေကို မကာကွယ်ပေးနိုင်ပါဘူး။ မိမိဟာ ကုမ္ပဏီရဲ့ VPN ကိုသုံးနေတယ် ဆိုရင် ကိုယ့်ရဲ့ အင်တာနက် အသုံးပြုမှုကို ကုမ္ပဏီကွန်ယက်ထိန်းချုပ်သူတွေက မြင်တွေ့ရပါလိမ့်မယ်။ တကယ်လို့ အပြင် စီးပွားဖြစ် VPN တစ်ခုကို ဝယ်သုံးနေတယ်ဆိုရင်လည်း အဲဒီဝန်ဆောင်မှုကို ထိန်းချုပ်သူတွေက ကိုယ့်အင်တာနက် အသုံးပြုမှုကို မြင်တွေ့နိုင်ပါလိမ့်မယ်။

မသမာတဲ့ VPN ဝန်ဆောင်မှုလုပ်ငန်းတွေကတော့ သုံးစွဲသူတွေရဲ့ ကိုယ်ရေးကိုယ်တာ သတင်းအချက်အလက် တွေနဲ့ အခြားတန်ဖိုးရှိတဲ့ အချက်အလက်တွေကို တမင်တကာ စောင့်ကြည့်ရယူခြင်း လုပ်တတ်ပါတယ်။

သုံးစွဲသူတွေ အင်တာနက်သုံးပြီး ပို့ထားတဲ့အချက်အလက်တွေကို အစိုးရနဲ့ ဥပဒေအရာရှိများက ကုမ္ပဏီ VPN ထိန်းချုပ်သူ သို့မဟုတ် အပြင်စီးပွားဖြစ် VPN လုပ်ငန်းတွေဆီကနေ တိုက်ရိုက်တောင်းတာမျိုး လုပ်လာနိုင် ပါတယ်။ ဒါ့ကြောင့် ကိုယ်အသုံးပြုတဲ့ VPN ဝန်ဆောင်မှုရဲ့ ကိုယ်ရေးကိုယ်တာလျှို့ဝှက်လုံခြုံမှုဆိုင်ရာ မူဝါဒတွေ ကိုပြန်လည်ဖတ်ကြည့်ပါ။ ကိုယ့်ရဲ့အချက်အလက်တွေကို VPN ဝန်ဆောင်မှုအနေနဲ့ ဘယ်လိုအခြေအနေမျိုးမှာ အစိုးရနဲ့ဥပဒေအရာရှိတွေထံကို ပေးခွင့်ရှိသလဲ သိအောင်လုပ်ပါ။

ဒါ့အပြင် VPN လုပ်ငန်းက ဘယ်နိုင်ငံတွေမှာ ဝန်ဆောင်မှုပေးသလဲ ဆိုတာကိုလည်း သိထားသင့်ပါတယ်။ လုပ်ငန်းအနေနဲ့ အစိုးရရဲ့ ပုဂ္ဂိုလ်ရေးရာသတင်းအချက်အလက် ထိန်းချုပ်မှုအပါအဝင် အဆိုပါနိုင်ငံတွေက ချမှတ်ထားတဲ့ ဥပဒေတွေကို လိုက်နာရမှာဖြစ်ပါတယ်။ ဥပဒေတွေက တစ်နိုင်ငံနဲ့တစ်နိုင်ငံ မတူပါဘူး။ အချို့ နိုင်ငံတွေမှာ မိမိရဲ့သတင်းအချက်အလက်တွေကို မိမိထံအသိပေးခြင်းမပြုဘဲတောင် အစိုးရက ရယူပိုင်ခွင့်ရှိပြီး အချို့နိုင်ငံတွေမှာတော့ အဲဒီလိုရယူမှုတွေကို မိမိကပြန်လည်အယူခံဝင်ပြီး ငြင်းဆိုလို့ရပါတယ်။ VPN လုပ်ငန်း တည်ရှိရာ နိုင်ငံနဲ့ ဥပဒေရေးရာ ကူညီထောက်ပံ့မှု သဘောတူညီချက် ချုပ်ဆိုထားတဲ့ နိုင်ငံတွေရှိရင် သတင်း အချက်အလက်တောင်းခံလာပါက လိုက်နာဆောင်ရွက်ရခြင်း ရှိနိုင်ကြောင်း သတိပြုပါ။

စီးပွားဖြစ် VPN ဝန်ဆောင်မှုအများစုကို ဝယ်ယူသုံးစွဲဖို့ဆိုရင် အကြွေးဝယ်ကဒ်အသုံးပြုပြီး ငွေပေးချေရလေ့ ရှိ ပါတယ်။ အကြွေးဝယ်ကဒ်မှာ မိမိဘယ်သူဘယ်ဝါဖြစ်တယ်ဆိုတာကို ခြေရာခံစေနိုင်တဲ့ အချက်အလက်တွေနဲ့ VPN ဝန်ဆောင်မှုလုပ်ငန်းကို အသိမပေးလိုတဲ့ အခြားကိုယ်ရေးအချက်အလက်တွေ ပါဝင်တတ်ပါတယ်။ ဒါကြောင့် ကိုယ့်ရဲ့ အကြွေးဝယ်ကဒ်နံပါတ်ကို VPN ဝန်ဆောင်မှုထံ ပေးမသိလိုလျှင် bitcoin သို့မဟုတ် လက်ဆောင်ကဒ်နဲ့ ငွေပေးချေမှုလက်ခံတဲ့ VPN ကိုရွေးသုံးပါ။ ဒါမှမဟုတ်ရင် ယာယီ သို့မဟုတ် ကြိုတင်ဖြည့် အကြွေးဝယ်ကဒ်နံပါတ်များ အသုံးပြုနိုင်ပါတယ်။ နောက်ထပ်သတိပြုရန်မှာ ခြေရာမခံနိုင်စေမယ့်နည်းနဲ့ ငွေပေးချေရင်တောင်

ကိုယ့်ရဲ့ IP လိပ်စာကို VPN က သိရှိနိုင်ပါတယ်။ ကိုယ့်ရဲ့ IP လိပ်စာကို VPN လုပ်ငန်းဆီ ကနေ လျှို့ဝှက်ထားချင်တယ်ဆိုရင် VPN နဲ့ချိတ်တဲ့အခါ Tor အသုံးပြုခြင်း သို့မဟုတ် အများသုံး Wi-Fi ကွန်ယက်ကနေ ချိတ်ဆက်ခြင်း ပြုလုပ်နိုင်ပါတယ်။

ကိုယ့်အတွက် အသင့်တော်ဆုံး VPN ကို ဘယ်လိုရွေးချယ်မလဲ။

လူတိုင်းမှာ VPN သုံးဖို့လိုတဲ့ ကိစ္စအမျိုးမျိုးရှိတတ်ပါတယ်။ VPN အမျိုးအစားနဲ့ အရည်အသွေးတွေဟာလည်း ဝန်ဆောင်မှု တစ်ခုနဲ့တစ်ခုကြား ကွာခြားမှုအများကြီး ရှိတတ်ပါတယ်။ ကိုယ့်အတွက် အသင့်တော်ဆုံး VPN ကို ရွေးချယ်ချင်တယ်ဆိုရင် အောက်ပါအချက်များအပေါ် အခြေခံပြီး VPN ဝန်ဆောင်မှုတွေကို နှိုင်းယှဉ်ကြည့် လို့ရပါတယ်။

ကြေညာချက်များ

VPN ဝန်ဆောင်မှုက သူ့ရဲ့ ကုန်စည်/ဝန်ဆောင်မှုနဲ့ ပတ်သက်ပြီး ဘာတွေကြေညာထားသလဲ။ သုံးစွဲသူတွေ ချိတ် ဆက်ဖို့အသုံးပြုတဲ့ အချက်အလက် တွေကို မကောက်ယူပါဘူး (အချက်အလက်ကောက်ယူခြင်းနှင့် ပတ်သက်၍ နောက်အပိုင်းတွင် ဆက်ဖတ်ပါ) သို့မဟုတ် ကောက်ယူထားတဲ့ အချက်အလက်တွေကို မျှဝေခြင်း၊ ပြန်လည် ရောင်းချခြင်း မပြုပါဘူးလို့ ကြေညာထားပါသလား။ ကြေညာချက်ဟာ အာမခံချက်နဲ့ မတူတာကြောင့် မှန်ကန် ကြောင်း သေချာအောင်စိစစ်ဖို့တော့ လိုပါတယ်။ VPN ဝန်ဆောင်မှုက ကိုယ့်ရဲ့အချက်အလက်တွေကို အခြား အပြင်ကုမ္ပဏီတွေဆီ တိုက်ရိုက်ရောင်းချခြင်းမပြုလျှင်တောင် အချက်အလက်တွေကို အသုံးချပြီး အခြား မည်သည့်နည်းဖြင့် ငွေရှာတယ်ဆိုတာကို သိအောင်လုပ်ပါ။ VPN ဝန်ဆောင်မှုရဲ့ ကိုယ်ရေးကိုယ်တာ လျှို့ဝှက် လုံခြုံမှုမူဝါဒများမှာ အသေးစိတ်ရှာဖွေဖတ်ကြည့်ပါ။

စီးပွားရေးမော်ဒယ်

VPN လုပ်ငန်းအနေနဲ့ သုံးစွဲသူတွေရဲ့ ကိုယ်ရေးအချက်အလက်တွေကို ပြန်မရောင်းဘူးဆိုရင်တောင်မှ အခြား တစ်နည်းနည်းနဲ့ လုပ်ငန်းရပ်တည်နိုင်ရန် လုပ်ဆောင်ရမှာဖြစ်ပါတယ်။ VPN ဝန်ဆောင်မှုဟာ သုံးစွဲသူတွေ ဆီကလည်း အခကြေးငွေမကောက်ဘူးဆိုရင် ဘယ်လိုနည်းနဲ့ သူ့ရဲ့လုပ်ငန်း ဆက်လက်လည်ပတ်နိုင်အောင် လုပ်သလဲ။ အလှူငွေနဲ့ ရပ်တည်နေသလား။ ဒီမေးခွန်းတွေကို ဖြေနိုင်ဖို့ သူ့ရဲ့ စီးပွားရေးမော်ဒယ်ကို သိဖို့လိုပါ တယ်။ တစ်ချို့ VPN တွေဟာ “freemium” မော်ဒယ် အသုံးပြုကြပါတယ်။ ဆိုလိုတာက စတင်သုံးစွဲချိန်မှာ အလကားပေးသုံး ပြီး သုံးစွဲမှုအတိုင်းအတာတစ်ခု ရောက်တဲ့အခါ အခကြေးငွေ စတင်ကောက်ခံပါတယ်။ ကိုယ့်မှာငွေကြေးအကန့်အသတ်ရှိတယ်ဆိုရင် ဒီလိုကိစ္စတွေကို သိထားသင့်ပါတယ်။

ဈေးကွက်တွင် နာမည်ရှိမှု

VPN လုပ်ငန်းနဲ့ ပတ်သက်တဲ့ ပုဂ္ဂိုလ်၊အဖွဲ့အစည်းများအကြောင်း စုံစမ်းသင့်ပါတယ်။ ဥပမာ VPN ဝန်ဆောင်မှု တစ်ခုကို ဆိုင်ဘာလုံခြုံရေးဆိုင်ရာ ကျွမ်းကျင်သူတွေက ထောက်ခံထားမှုရှိပါသလား။ VPN နဲ့ ပတ်သက်ပြီး ရေးထားတဲ့ သတင်းတွေရှိသလား။ VPN လုပ်ငန်းတစ်ခုဟာ သတင်းအချက်အလက်လုံခြုံမှုဆိုင်ရာ နယ်ပယ်မှ နာမည်ရှိသူတွေက တည်ထောင်ထားတာဆိုရင် ပိုပြီးယုံကြည်လို့ရနိုင်လောက်ပါတယ်။ ဘယ်သူမှ ထောက်ခံမှု မလုပ်လိုတဲ့ VPN ဝန်ဆောင်မှုတွေ၊ သက်ဆိုင်ရာနယ်ပယ်မှာ ဘယ်သူမှမသိသူတွေက တည်ထောင်ထားတဲ့ VPN လုပ်ငန်းတွေဖြစ်နေရင် သတိထားပါ။

အချက်အလက်ကောက်ယူမှု

အချက်အလက်ကို အစကတည်းက ကောက်ယူမှုမလုပ်ဘူးဆိုရင် ပြန်ရောင်းလို့လည်းမရပါဘူး။ ကိုယ်ရေး ကိုယ်တာ လျှို့ဝှက်လုံခြုံမှု မူဝါဒ ဖတ်တဲ့အချိန်မှာ VPN က သုံးစွဲသူတွေရဲ့ အချက်အလက်တွေကို ကောက်ယူ ခြင်းရှိမရှိလည်း စစ်ဆေးပါ။ သုံးစွဲသူအချက်အလက်တွေကို ကောက်ယူခြင်းမရှိပါဟု အတိအလင်းကြေညာခြင်း မရှိပါက ကောက်ယူဖို့များပါတယ်။ ထို့အပြင် နေရာဒေသအပေါ်မူတည်ပြီး အစိုးရတွေကလည်း ကောက်ယူထား တဲ့အချက်အလက်တွေကို တောင်းခံခြင်း၊ တရားရုံးအမိန့်နဲ့ သိမ်းဆည်းခြင်းတို့ လုပ်နိုင်ပါတယ်။

ကုမ္ပဏီက ချိတ်ဆက်မှုအချက်အလက်များ ကောက်ယူခြင်းမပြုဟု ကြေညာထားလျှင်တောင် အမှန်တကယ် လိုက်နာသည်ဟု အာမမခံနိုင်ပါ။ ဒါ့ကြောင့် သတင်းမီဒီယာထဲမှာ VPN နဲ့ပတ်သက်ပြီး ဖော်ပြထားတာရှိသလား စုံစမ်းကြည့်သင့်ပါတယ်။ သုံးစွဲသူတွေကို လိမ်လည်လှည့်ဖျားတာမျိုး လုပ်ဖူးရင် သတင်းထဲမှာ ပါနိုင်ပါတယ်။ သံသယဖြစ်စရာ ကိစ္စတွေရှိနေခဲ့မယ်ဆိုရင် နည်းနည်းရှာကြည့်ရုံနဲ့ ကိုယ့်အတွက် အကျိုးရှိနိုင်ပါတယ်။

တည်နေရာနှင့် ဥပဒေများ

VPN လုပ်ငန်းတစ်ခုဟာ ဘယ်နေရာမှာ အခြေစိုက်သလဲဆိုတာလည်း အရေးကြီးပါတယ်။ ဝန်ဆောင်မှုကို ရွေးချယ်တဲ့ အခါမှာ အခြေစိုက်ရာ နိုင်ငံ ရဲ့ သတင်းအချက်အလက်လျှို့ဝှက်လုံခြုံမှုဆိုင်ရာ ဥပဒေတွေက အရေးကြီးသလို မူဝါဒနဲ့ဥပဒေတွေ အပြောင်းအလဲရှိနိုင်တာကိုလည်း သတိပြုပါ။

ကုဒ်ဖြင့်ပြောင်းလဲခြင်း

VPN တစ်ခုရဲ့ ကုဒ်ဖြင့်ပြောင်းလဲမှုဟာ ဘယ်လောက်လုံခြုံမှုရှိသလဲ။ အကယ်၍ Point-to-Point Tunneling Protocol (PPTP) သို့မဟုတ် အားနည်းတဲ့ ကုဒ်ဖြင့်ပြောင်းလဲမှု ကုဒ်များ အသုံးပြုခဲ့မယ်ဆိုရင် VPN ကနေတစ် ဆင့် ဖြတ်သန်းသွားတဲ့ အချက်အလက်တွေကို မိမိရဲ့ ISP

သို့မဟုတ် အစိုးရကနေ အလွယ်တကူ ပြန်ဖြည်ပြီး ဖတ်ရှုနိုင်မှာဖြစ်ပါတယ်။ ကိုယ်က ရုံးရဲ့ VPN ကို အသုံးပြုနေတယ်ဆိုရင် အိုင်တီဌာနကို ဆက်သွယ်ပြီး အင်တာနက်ချိတ်ဆက်မှု ဘယ်လောက်လုံခြုံမှုရှိသလဲဆိုတာကို မေးမြန်းစုံစမ်းပါ။ VPN ဝန်ဆောင်မှုတွေရဲ့ ကုဒ်ဖြင့်ပြောင်းလဲမှု မည်မျှခိုင်မာသလဲဆိုတာကို နှိုင်းယှဉ်အကဲခတ်ဖို့ ခက်ခဲနိုင်တာကြောင့် One Privacy Site က ထုတ်ထားတဲ့ ဤ VPM နှိုင်းယှဉ်မှုဇယား ကို ကြည့်ကြည့်ပါ။ ဒီဇယားမှာ အခြေစိုက်ရာ နိုင်ငံတွေနဲ့ သက်ဆိုင် ရာမူဝါဒတွေအပေါ် အခြေခံပြီး VPN ဝန်ဆောင်မှု ၂၀၀ နီးပါးကို နှိုင်းယှဉ်သုံးသပ်ပြထားပါတယ်။

EFF အနေနဲ့ကတော့ VPN နှိုင်းယှဉ်အမှတ်ပေးမှုတွေကို အာမမခံနိုင်ပါဘူး။ အလွန်ကောင်းမွန်တဲ့ ကိုယ်ရေး အချက်အလက်လျှို့ဝှက်လုံခြုံမှုမူဝါဒတွေ ရှိနေပေမယ့်လည်း VPN ဝန်ဆောင်မှုရဲ့ ထိန်းချုပ်သူတွေက မသမာ တာမျိုး ရှိနိုင်ပါတယ်။ ဒါ့ကြောင့် ကိုယ်မယုံကြည်ရဘူးထင်တဲ့ VPN ဆိုရင် မသုံးပါနဲ့။

ဘယ် VPN ကမှတော့ အလုံးစုံပြီးပြည့်စုံတယ်ဆိုတာ မရှိပါဘူး။ VPN တစ်ခုရွေးချယ်တဲ့အခါမှာ စဉ်းစားစရာ ကိစ္စများစွာရှိပါတယ်။ ကိုယ့်ရဲ့ဒစ်ဂျစ်တယ်လုံခြုံရေးအတွက် အသုံးပြုဖို့နည်းပညာတစ်ခုကို မရွေးချယ်မီမှာ မိမိရဲ့ လုံခြုံရေးအစီအစဉ် နဲ့ အမြဲတစ်စေ ပြန်ချိန်ညှိပြီး သုံးသပ်ပါ။