လူအခွင့်အရေးတက်ကြွလှုပ်ရှားသူများအတွက် ဒီဂျစ်တယ်လုံခြုံရေးလမ်းညွှန်

မာတိကာ

နိဒါန်း

ဒစ်ဂျစ်တယ်ကမ္ဘာနဲ့ ရုပ်ပိုင်းဆိုင်ရာကမ္ဘာရဲ့ ပိုင်းခြားထားတဲ့ နယ်နိမိတ်ဟာ တစ်နေ့ထက်တစ်နေ့ ပိုပြီးတော့ ကျဉ်းမြောင်းလာပါတယ်။ ကျွန်တော်တို့ရဲ့ နေအိမ်တွေ၊ အလုပ်နေရာတွေ၊ ကိုယ်ခန္ဓာတွေနဲ့ ဝိသေသ လက္ခဏာ တွေတောင်မှ ဆက်သွယ်ထားတဲ့ ဒီကွန်ရက်ကြီးထဲမှာ ရောယှက်နေပါပြီ။ မျက်နှာပြင်တစ်ခုကို တို့ထိလိုက်ရုံနဲ့ အရာရာဟာ လွယ်ကူမြန်ဆန်ပြီး အကျိုးရှိမယ်ဆိုတာမျိုးကိုတောင် ဒီဒစ်ဂျစ်တယ်ကမ္ဘာကြီးက အာမခံပေးထားပါတယ်။ ဒါပေမဲ့ ဒီအဆင်ပြေတယ်ဆိုတဲ့ အယောင်ဆောင်မှု ဒါမှမဟုတ် စိတ်ကူးယဉ်မှုရဲ့ နောက်ကွယ်မှာ ဖော်ထုတ်ဖို့ လိုအပ်တဲ့ ပိုပြီးတော့ နက်နဲတဲ့၊ ပိုပြီး ကြောက်စရာကောင်းတဲ့ ဇာတ်လမ်းတစ်ပုဒ် ရှိနေပါတယ်။

ဒီနည်းပညာတွေဟာ သူ့သဘာဝအတိုင်းရှိနေတဲ့ ဘက်မလိုက် ကိရိယာတွေ မဟုတ်ပါဘူး။ အဲဒီကနေ စပြော ရမယ်ဆိုရင် သူတို့ဟာ လက်ရှိ အာဏာအခြေပြုစနစ်တွေရဲ့ လက်တံတွေပဲ ဖြစ်ပါတယ်။ နည်းအမျိုးမျိုးနဲ့ ဒီနည်းပညာတွေကို ငွေကြေးအကျိုးစီးပွားအတွက် ရည်ရွယ်ပြီး ဒီဇိုင်းဆွဲ၊ ဖြန့်ကျက်ပြီး ပျံနှံစေပါတယ်။ ကျွန်တော်တို့ရဲ့ နေအိမ်တွေမှာရှိတဲ့ နည်းပညာမြင့်ကိရိယာတွေဟာ ကျွန်တော်တို့ရဲ့ အပြုအမူကို ခန့်မှန်းဖို့၊ လွှမ်းမိုးဖို့နဲ့ နောက်ဆုံးမှာတော့ ဒီအပြုအမူတွေကိုသုံးပြီး ငွေကြေးအကျိုးအမြတ်အဖြစ် ပြောင်းလဲဖို့အတွက် ကိုယ်ရေးကိုယ်တာ အချက်အလက်တွေကို စုဆောင်း နေပါတယ်။ ကျွန်တော်တို့ရဲ့ ကျန်းမာရေးကို စောင့်ကြည့်ပေးဖို့ ဝတ်ဆင်နိုင်တဲ့ပစ္စည်းတွေ (wearables) ဟာ အာမခံကုမ္ပဏီတွေရဲ့ ငွေကြေးအကျိုးအမြတ် ထုတ်ယူဖို့ နောက်ထပ် သတင်းအချက်အလက်စုဆောင်းရာ နေရာတစ်ခု ဖြစ်လာပါတယ်။ အလုပ်ပြီးမြောက်ဖို့ရာ အထောက်အကူပေးတဲ့ အက်ပ် (app)တွေဟာ အလုပ်ရှင်တွေအတွက် စောင့်ကြည့်ရေးစနစ်တွေအဖြစ် နှစ်ဆတိုး လုပ်ဆောင်နေပါတယ်။ ပြီးတော့ ဇီဝဆိုင်ရာ အချက်အလက် စုဆောင်းတဲ့စနစ်တွေ (biometric systems) ဟာ ကျွန်တော်တို့ ကမ္ဘာကြီးထဲမှာ လူပ်ရှားသွားလာနိုင်ဖို့အတွက် ကျွန်တော်တို့ရဲ့ခန္ဓာကိုယ်တွေကို စက်တွေက ဖတ်ရှုလို့/ခွင့်ရနေရမယ်ဆိုတဲ့ အယူအဆကို နေသားကျအောင် လုပ်နေပါတယ်။

လုံခြုံရေးဆိုတာ စုပေါင်းလိုအပ်ချက်တစ်ခု ဖြစ်ပါတယ်။ ဒါဟာ ဒစ်ဂျစ်တယ်ကမ္ဘာနဲ့ ရုပ်ပိုင်းဆိုင်ရာကမ္ဘာ နှစ်ခုစလုံးမှာ ဖိနှိပ်မှု၊ ထုတ်ယူ၊ထိန်းချုပ်မှုတွေကို ဆန့်ကျင်တဲ့ ခုခံတော်လှန်မှုတစ်ခု ဖြစ်ပါတယ်။ ဒါကြောင့် ဒီအခြေခံလမ်းညွှန်ကို ပုံစံမျိုးစုံနဲ့ မတရားမှုကို ဆက်လက် ခုခံတော်လှန်နေကြတဲ့၊ မကြာခဏဆိုသလို ကြီးမားတဲ့ အန္တရာယ်တွေကို ရင်ဆိုင်နေရတဲ့ လူ့အခွင့်အရေး လှုပ်ရှားသူတွေကို ကျွန်တော်တို့က ရည်စူးရေးသားပါတယ်။ ဒါ့အပြင် သူတို့ရဲ့ နေ့စဉ်ရုန်းကန်မှုတွေကို မကြာခဏဆိုသလို လျစ်လျူရှုခံနေရပေမဲ့ လွတ်လပ်မှု၊ ဂုဏ်သိက္ခာနဲ့ တန်းတူညီမျှမှုအတွက် လှုပ်ရှားမှုတိုင်းရဲ့ ကျောရိုးအဖြစ် ရပ်တည်နေကြတဲ့ အလုပ်သမားလူတန်းစားများစွာကိုလည်း ဂုဏ်ပြုအပ်ပါတယ်။

ဒီအခြေခံလမ်းညွှန်ဟာ ထူထုလှုပ်ရှားမှုအတွက်၊ အောက်မေ့ဖွယ်ရာများ အတွက်၊ ပြီးတော့ လွတ်လပ်မှု အတွက် အထောက်အကူတစ်ခု ဖြစ်ပါစေ။

ဤလမ်းညွှန်အကြောင်း ဖော်ပြချက်

ဤလမ်းညွှန်သည် အချို့သော တက်ကြွလှုပ်ရှားသူများကို ထိခိုက်စေနိုင်သည့် ဒစ်ဂျစ်တယ်လုံခြုံရေးဆိုင်ရာ ခြိမ်းခြောက်မှုများကို ဖော်ပြထားသည့် သုတေသနစာတမ်းတစ်ခုသာ ဖြစ်သည်။ ဤစာတမ်းသည် ဆောင်ရန်၊ ရှောင်ရန်များကို ပြဋ္ဌာန်းထားသည့် စာရွက်စာတမ်းမဟုတ်ပါ။ ခြိမ်းခြောက်မှုပုံစံတိုင်းသည် မတူညီကွဲပြား၊ ပြောင်းလဲနေပြီး၊ အခြေအနေအပေါ်မူတည်နေသောကြောင့် ဤစာတမ်းပါ အကြံပြုချက်အားလုံးသည် အဆိုပြုချက်များသာ ဖြစ်ပါသည် ။ ဤစာတမ်းကို အစပျိုးလေ့လာရန်အတွက်သာ အသုံးပြုပြီး၊ စံနမူထားပြီး ဆောက်ရွက်စစ်ဆေးရန် စာရင်းအဖြစ် မသတ်မှတ်ပါနှင့်။

ဤလမ်းညွှန်သည် ကျွန်ုပ်တို့ရှေ့မှ ဒစ်ဂျစ်တယ်လုံခြုံရေးနယ်ပယ်တွင် လုပ်ကိုင်ခဲ့ကြသူများ၏ ကြီးမားသော ကြိုးပမ်းအားထုတ်မှုများအပေါ် အခြေခံထားခြင်း ဖြစ်သည်။ သူတို့၏ ကြိုးပမ်းအားထုတ်မှုများ၊ ရဲစွမ်းသတ္တိများနှင့် အာဏာကို ရင်ဆိုင်ရာတွင် အရှုံးမပေးနောက်မဆုတ်ခြင်းတို့အတွက် ကျွန်ုပ်တို့ လေးစားဂါရဝပြုပါသည်။ လုံခြုံရေးသည် တစ်သက်တာလုံး လေ့ကျင့်နေရမည့် အရာဖြစ်သောကြောင့် ကျွန်ုပ်တို့သည် ၎င်းတို့ထံမှ သင်ယူခြင်း၊ အခြေအနေအရ လိုက်လျောညီထွေဖြစ်အောင် ပြုလုပ်ခြင်းနှင့် ဆက်လက်လက်ဆင့်ကမ်းခြင်းတို့ကို ပြုလုပ်နေပါသည်။

ဤစာရွက်စာတမ်းသည် လူတိုင်းအတွက် လမ်းညွှန်ချက် အစုံအလင်ကို ပေးထားခြင်းမရှိသည့်အပြင် လက်တွေ့လုပ်ဆောင်ရသည့် သင်တန်းများ၊ ဖောက်ထွင်းဝင်ရောက်နိုင်မှု စမ်းသပ်စစ်ဆေးခြင်းများ သို့မဟုတ် အတတ်ပညာရှင်တို့ရဲ့ လုံခြုံရေး အကဲဖြတ်ချက်များကို အစားထိုးနိုင်မည် မဟုတ်ပါ။ ခြိမ်းခြောက်မှု အခြေအနေသည် နေ့စဉ်နှင့်အမျှ ပြောင်းလဲနေသောကြောင့် ၎င်းခြိမ်းခြောက်မှုကို အချိန်နှင့်တစ်ပြေးညီ နောက်ဆုံး အခြေအနေအတိုင်း ထားရှိနိုင်မည် မဟုတ်သောကြောင့် စာတမ်းပါအကြောင်းအရာများကို သင်ဖတ်ပြီးသည့်အချိန်တွင် ခေတ်နောက်ကျနေနိုင်သည်ဟု အသိပေးလိုပါသည် ။

မသက်ဆိုင်ကြောင်းရှင်းလင်းချက်

ဤစာတမ်းပါ မည်သည့်အရာမျှ ဥပဒေအကြံဉာဏ်၊ ပညာရပ်ဆိုင်ရာလုံခြုံရေး အကြံပေးချက် သို့မဟုတ် သီးခြားလုပ်ဆောင်မှုတစ်ခုခုကို ထောက်ခံခြင်းအဖြစ် မယူဆစေလိုပါ။ ဤအကြောင်းအရာများသည် ပညာရေး နှင့် သတင်းအချက်အလက်ဆိုင်ရာ ရည်ရွယ်ချက်များအတွက်သာ 'ရှိရင်းစွဲအတိုင်း' ပေးထားခြင်းဖြစ်သည်။ စာဝှက်စနစ်၊ စောင့်ကြည့်မှု၊ သတင်းအချက်အလက်ထိန်းသိမ်းမှုနှင့် ဒစ်ဂျစ်တယ်လှုပ်ရှားမှုဆိုင်ရာ ဥပဒေများသည် တရားစီရင်ပိုင်ခွင့်အလိုက် ကွဲပြားပြီး အချိန်နှင့်အမျှ ပြောင်းလဲနေပါသည်။ မည်သည့်အကြံပြုချက်ကိုမဆို အကောင်အထည်မဖော်မီ ၎င်း၏တရားဝင်မှုနှင့်ပတ်သက်၍ အရည်အချင်းပြည့်မီသော ရှေ့နေများနှင့် တိုင်ပင်ဆွေးနွေးပြီး သင်ရွေးချယ်ထားသော ကိရိယာများသည် သင့်လုပ်ငန်းလည်ပတ်ရာနေရာတွင် တရားဝင်မှုရှိမရှိကို သေချာစစ်ဆေးပါ။ အချို့သော တရားစီရင်ပိုင်ခွင့်များတွင် အချို့သော စာဝှက်စနစ်သို့မဟုတ် အမည်ဝှက်ဆော့ဖ်ဝဲလ်များကို ကန့်သတ်ထားခြင်း သို့မဟုတ် တားမြစ်ထားခြင်းများ ရှိပါသည်။ လုံခြုံရေးဆော့ဖ်ဝဲလ် သို့မဟုတ် စာဝှက်ကုဒ်များကို သင်နှင့်အတူ ယူဆောင်သွားရန် သို့မဟုတ် မျှဝေရန် စီစဉ်ပါက ပို့ကုန်ထိန်းချုပ်ရေး စည်းမျဉ်းများကို သေချာအကဲဖြတ်ပါ။

ဤစာတမ်းကို အခြေခံ၍ ဆောင်ရွက်ခဲ့သော သို့မဟုတ် မဆောင်ရွက်ခဲ့သော လုပ်ဆောင်မှုများအတွက် ဖြစ်ပေါ်လာသော တာဝန်များသည် စာရေးသူများနှင့် မသတ်ဆိုင်ပါ။ သင်၏ကိုယ်ပိုင်ဆုံးဖြတ်ချက်ကို အသုံးပြုပါ၊ ကျွမ်းကျင်သူ၏အကြံဉာဏ်ကို ရယူပြီး မည်သည့်လုံခြုံရေးအစီအမံမျှ စင်းလုံးချောကောင်းမွန်မည် မဟုတ်သည်ကို သတိရပါ။

ဤစာတမ်း၌ hyperlink များကို ၂၀၂၅ ခုနှစ်၊ ဇူလိုင်လ ၁၆ ရက်နေ့အထိ စမ်းသပ်စစ်ဆေးပြီး အသုံးပြုနိုင်ကြောင်း တွေ့ရှိရသော်လည်း ဝဘ်ဆိုဒ်ပါအကြောင်းအရာများသည် ဆိုက်ပိုင်ရှင်များ၏ ဆုံးဖြတ်ချက်အရ ပြောင်းလဲနိုင်သောကြောင့် ၎င်းတို့ဆက်လက်အသက်ဝင်နေမည်ကို ကျွန်ုပ်တို့အာမခံနိုင်မည် မဟုတ်ပါ။ ဤစာရွက်စာတမ်းကို အသုံးပြုခြင်းသည် သင့်ကိုယ်ပိုင်အန္တရာယ်ဖြင့်သာ ဖြစ်သည်။

စာရေးသူများအကြောင်း

ဂျင် လီနစ်-ဒင်ကို **(Jean Linis-Dinco, PhD)** သည် ဖိလစ်ပိုင်နိုင်ငံမှ လူ့အခွင့်အရေး တက်ကြွလှုပ်ရှားသူတစ်ဦး ဖြစ်သည်။ Jean သည် UNSW (University of New South Wales) မှ ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ ပါရဂူဘွဲ့ကို ရရှိခဲ့ပြီး မြန်မာနိုင်ငံရှိ ရိုဟင်ဂျာအရေးအခင်းတွင် မှားယွင်းသော/အချက်အလက်မှန်မဟုတ်သော သတင်းများ၏ကဏ္ဍကို အဓိကထား၍ သုတေသနပြုခဲ့သည်။ နည်းပညာနှင့် လူ့အခွင့်အရေးနယ်ပယ်တွင် Jean ၏ လုပ်ဆောင်မှုများကို ၂၀၂၂ ခုနှစ်တွင် Women in AI Ethics™ (WAIE) က ကမ္ဘာတစ်ဝန်းရှိ ထိပ်တန်း အမျိုးသမီး ၁၀၀ စာရင်းတွင် ထည့်သွင်းဂုဏ်ပြုခဲ့သည်။ Jean သည် လက်ရှိတွင် Manushya Foundation တွင် အကြီးတန်း ဒစ်ဂျစ်တယ် အခွင့်အရေး အကြံပေးအရာရှိအဖြစ် လုပ်ကိုင်နေပါသည်။

ဂျာဂါနာ ဇဗက်ကိုဗာ **(Gergana Tzvetkova, PhD)** သည် သုတေသီတစ်ဦးဖြစ်ပြီး Counterintuitive Institute ကို ပူးတွဲတည်ထောင်သူတစ်ဦးလည်း ဖြစ်သည်။ Counterintuitive Institute သည် အကြမ်းဖက်မှု ပုံစံသစ်များကို လေ့လာခြင်းနှင့် တန်ပြန်ခြင်း၊ အနှစ်သာရရှိသော တန်းတူညီမျှမှု၊ အမျိုးသမီးအခွင့်အရေးများ နှင့် အမျိုးသမီးတို့အတွက် နည်းပညာများ၊ ကျင့်ဝတ်ဆိုင်ရာ နည်းပညာများကို မြှင့်တင်ရန် လုပ်ဆောင်နေသည့် ဘူလ်ဂေးရီးယားအခြေစိုက် အစိုးရမဟုတ်သောအဖွဲ့အစည်းတစ်ခုဖြစ်သည်။ လူ့အခွင့်အရေးနယ်ပယ်တွင် ၁၂ နှစ်ကျော် အတွေ့အကြုံရှိသော Gergana သည် ကျားမအခြေပြုအကြမ်းဖက်မှု၊ အမျိုးသမီးများအပေါ် ဆိုက်ဘာအကြမ်းဖက်မှု၊ ကျားမအခြေပြု သတင်းမှားများ ၊ ဒစ်ဂျစ်တယ်ကိုကောင်းမွန်စွာ အသုံးပြုနိုင်ရေး သင်းကြားပေးခြင်း နှင့် ဒစ်ဂျစ်တယ်အခွင့်အရေးဆိုင်ရာ သုတေသနပြုလုပ်မှုများကို ဦးဆောင်ကာ ပါဝင်ကူညီခဲ့ပါသည်။

မြန်မာပြန်ဆိုသူ

နောင်နောင် (**Naung Naung**) သည် University of Sydney မှ လူမှုတရားမျှတမှုဆိုင်ရာ မဟာဘွဲ့လေ့လာနေသူ တစ်ဦးဖြစ်သည်။ မြန်မာနိုင်ငံသားဖြစ်ပြီး ၂၀၂၁ ခုနှစ်တွင် ဩစတြေးလျသို့ ပြောင်းရွှေ့အခြေချနေထိုင်ခဲ့သည်။ လက်ရှိတွင် ကုလသမဂ္ဂ စီမံကိန်းဝန်ဆောင်မှုရုံး (UNOPS) တွင် အကြံပေးအဖြစ် လုပ်ကိုင်နေသည်။ လူသားချင်း စာနာထောက်ထားမှုနှင့် ဖွံ့ဖြိုးတိုးတက်ရေးဆိုင်ရာ အတွေ့အကြုံ များစွာကို ရှိပြီး အထူးသဖြင့် စီမံကိန်းစီမံခန့် ခွဲမှု တို့တွင် အတွေ့အကြုံများစွာရှိသည်။ ၂၀၂၁ ခုနှစ် မြန်မာနိုင်ငံ စစ်အာဏာသိမ်းပြီးနောက်တွင် ၎င်း၏စိတ်ဝင်စား မှုသည် လူမှုတရားမျှတမှု၊ အိုးအိမ်စွန့်ခွာရွှေ့ပြောင်း နေထိုင်မှု၊ နိုင်ငံဖြတ်ကျော် တတ်ကြွလှုပ်ရှားမှုနှင့် အာဏာရှင်စနစ်လွန် အုပ်ချုပ်ရေးဆိုင်ရာ ပညာရပ်ဆိုင်ရာ သုတေသန များဘက်သို့ ပြောင်းလဲလာခဲ့သည်။

ရှုပ်ပိုင်း

ဤ ဒီဂျစ်တယ်လုံခြုံရေးလမ်းညွှန်ကို Global Campus Alumni ၂၀၀၄-၂၀၀၅ ခုနှစ် စီမံချက်များ ၏ တစ်စိတ်တစ်ပိုင်းအဖြစ် ဥရောပသမဂ္ဂ၏ ပံ့ပိုးမှုဖြင့် ရေးဆွဲခဲ့ပါသည်။

Co-funded by the European Union

Global Campus Alumni

Together for Human Rights

အတိုကောက်စာလုံးများ

- **2FA** – Two Factor Authentication (အဆင့်နှစ်ဆင့်ဖြင့် အတည်ပြုခြင်း)
- **AES** - Advanced Encryption Standard (အဆင့်မြင့် စာဝှက်လျှို့ဝှက်ကုဒ်စနစ်)
- **DES** - Data Encryption Standard (အချက်အလက် စာဝှက်လျှို့ဝှက်ကုဒ်စနစ်)
- **DNS** – Domain Name System (ဒိုမိန်း (Domain) အမည်များကို အိုင်ပီလိပ်စာ (IP) များအဖြစ် ပြောင်းလဲပေးသည့်စနစ်)
- **DNSSEC** - Domain Name System Security Extensions (ဒိုမိန်း (Domain) အမည်များကို အိုင်ပီလိပ်စာ (IP) များအဖြစ် ပြောင်းလဲပေးသည့်စနစ်လုံခြုံရေး တိုးချဲ့မှုများ)
- **DoH** – DNS over HTTPS (HTTPS ပေါ်မှ DNS)
- **DoT** – DNS over TLS (TLS ပေါ်မှ DNS)
- **DPI** – Deep Packet Inspection (အချက်အလက်များကို အသေးစိတ်စစ်ဆေးခြင်း)
- **ECC** - Elliptic-curve cryptography (ဘဲဥပုံမျဉ်းကွေးသုံး စာဝှက်စနစ်)
- **EDRi** - European Digital Rights (ဥရောပဒစ်ဂျစ်တယ်အခွင့်အရေး)
- **EFF** – Electronic Frontiers Foundation (အီလက်ထရွန်နစ်နယ်နိမိတ် ဖောင်ဒေးရှင်း)
- **EXIF** – Exchangeable File Format (ဖလှယ်နိုင်သော ဖိုင်ပုံစံ)
- **FLD** – Front Line Defenders (ရှေ့တန်းကာကွယ်သူများ)
- **GEC** – Global Encryption Coalition (ကမ္ဘာလုံးဆိုင်ရာ စာဝှက်စနစ်ညွှန့်ပေါင်းအဖွဲ့)
- **GPS** – Global Positioning System (ကမ္ဘာလုံးဆိုင်ရာ တည်နေရာပြစနစ်)
- **HTTP/S**- Hypertext Transfer Protocol/ Secure (လုံခြုံသော စာသားအပြန်အလှန်ပို့စနစ်)
- **IDEA** - International Data Encryption Algorithm (နိုင်ငံတကာဒေတာ စာဝှက်စနစ်)
- **Infosec**- Information Security (သတင်းအချက်အလက် လုံခြုံရေး)
- **ISP** – Internet Service Providers (အင်တာနက်ဝန်ဆောင်မှုပေးသူများ)
- **MFA** - Multi-factor authentication (အချက်များစွာဖြင့် စစ်မှန်ကြောင်း အတည်ပြုခြင်း)
- **NSA** - National Security Agency (အမျိုးသားလုံခြုံရေးအေဂျင်စီ)
- **OpenPGP** - Open PGP (ပွင့်လင်းသော ကောင်းမွန်သည့် ကိုယ်ရေးကိုယ်တာလုံခြုံမှု)
- **OPSEC** – Operational Security (လုပ်ငန်းလည်ပတ်မှု လုံခြုံရေး)
- **OS** – Operating System (ကွန်ပျူတာစက်လည်ပတ်ရေးစနစ်)
- **PDF** – Portable Document Format (သယ်ဆောင်ရလွယ်ကူသော စာရွက်စာတမ်းပုံစံ)
- **PGP** – Pretty Good Privacy (ကောင်းမွန်သော ကိုယ်ရေးကိုယ်တာလုံခြုံမှု)

- **SCF** – Secure Communication Framework (လုံခြုံသော ဆက်သွယ်ရေးမူဘောင်)
- **SOCKS** – Socket Secure (ဆော့ခ်ကတ် လုံခြုံရေး)
- **USB** - Universal Serial Bus (ယူအက်စ်ဘီ)
- **VPN** – Virtual Private Network (ကိုယ်ပိုင်ကွန်ရက်အတု)

အပိုင်း ၁: နိဒါန်း

အဓိပ္ပာယ်ဖွင့်ဆိုချက်

အပြည်ပြည်ဆိုင်ရာဆက်သွယ်ရေး သမဂ္ဂ (International Telecommunications Union) က ဆိုက်ဘာလုံခြုံရေးကို "ဆိုက်ဘာပတ်ဝန်းကျင်နှင့် အဖွဲ့အစည်းများ၊ အသုံးပြုသူများ၏ ပိုင်ဆိုင်မှုများကို ကာကွယ်ရန်အတွက် အသုံးပြုနိုင် သော ကိရိယာများ၊ မူဝါဒများ၊ လုံခြုံရေးဆိုင်ရာ အယူအဆများ၊ လုံခြုံရေး အကာအကွယ်များ၊ လမ်းညွှန်ချက်များ၊ အန္တရာယ်စီမံခန့်ခွဲမှုချဉ်းကပ်ပုံများ၊ လုပ်ဆောင်ချက်များ၊ လေ့ကျင့်ရေးသင်တန်းများ၊ အကောင်းဆုံး အလေ့အကျင့်များ၊ အာမခံချက်များနှင့် နည်းပညာများ စုစည်းမှု" အဖြစ် အဓိပ္ပာယ်ဖွင့်ဆိုထားသည်[1]။ ဤအဓိပ္ပာယ်ဖွင့်ဆိုချက်သည် ဆိုက်ဘာလုံခြုံရေး၏ နည်းပညာနှင့် လုပ်ငန်းစဉ်ဆိုင်ရာ ရှုထောင့်များကို ထည့်သွင်းစဉ်းစားထားသော်လည်း ဒစ်ဂျစ်တယ်လောက၏ ပိုမိုနက်ရှိုင်းသော လူမှုရေး၊ နိုင်ငံရေးနှင့် ရုပ်ဝတ္ထုဆိုင်ရာ အခြေအနေများကို ဖော်ပြရန် ပျက်ကွက်နေသည်။ ဆိုက်ဘာလုံခြုံရေးသည် အဖွဲ့အစည်းများ သို့မဟုတ် အသုံးပြုသူများ၏ ပိုင်ဆိုင်မှုများကို ကာကွယ်ရန်အတွက်သာ မဟုတ်ပါ။ အမှန်စင်စစ်၊ ဤအဓိပ္ပာယ်ဖွင့်ဆိုချက်သည် နိုင်ငံတော်၊ စီးပွားရေးလုပ်ငန်းစုများနှင့် စစ်ဘက်၊ စစ်ရေးဆိုင်ရာ လက်နက်ကိရိယာများ ထုတ်လုပ်ဖြန့်ချိသော စက်မှုလုပ်ငန်းစုကြားက ဆက်စပ်ရှုပ်ထွေးသော ဆက်ဆံရေးတို့ ထံမှ ခြိမ်းခြောက်မှုများကို အခံရဆုံးဖြစ်သည့် လူများနှင့် လူမှုအသိုင်းအဝိုင်း၏ နေ့စဉ်ဘဝကို လျစ်လျူရှုလေ့ရှိသော လစ်ဘရယ်အသစ်ဝါဒီ ၊ ပုဂ္ဂလဓိဋ္ဌာန်ဝါဒီ၊ ငွေကြေးအကျိုးအမြတ် စီးပွားရေးဆန်လွန်းသော ရှုထောင့်ကို အားဖြည့်ပေးသည်။

ဒစ်ဂျစ်တယ်လုံခြုံရေး၊ ဆိုက်ဘာလုံခြုံရေးနှင့် သတင်းအချက်အလက်လုံခြုံရေးတို့သည် ဒစ်ဂျစ်တယ်ပတ်ဝန်းကျင်ရှိ အချက်အလက်များ၊ စနစ်များနှင့် အသုံးပြုသူများကို ကာကွယ်သည့် အယူအဆကို ဖော်ပြရန်အတွက် တစ်ခုနှင့်တစ်ခု အပြန်အလှန်လဲလှယ်ကာ မကြာခဏ အသုံးပြုလေ့ရှိသည့် စကားလုံးများဖြစ်သည်။ ဝေါဟာရတစ်ခုစီတွင် ၎င်း၏ ကိုယ်ပိုင်မူလဇစ်မြစ်နှင့် အလေးပေးမှုများရှိသော်လည်း လက်တွေ့တွင် ဤခြားနားချက်များသည် မှုန်ဝါးသွားတတ် ပါသည်။ ဝေါဟာရသမိုင်းနှင့်ပတ်သက်၍ အတွေးအခေါ်ဆိုင်ရာ ငြင်းခုံမှုများတွင် ပါဝင်ရန် ကျွန်ုပ်တို့ စိတ်ဝင်စားသော်လည်း ဤလမ်းညွှန်သည် ထိုရည်ရွယ်ချက်မှ ခွဲထွက်ပြီး လက်တွေ့ကျသော ချဉ်းကပ်မှုကိုသာ အာရုံစိုက်ထားသည်။ ရှင်းလင်းပြတ်သားမှုနှင့် ရှေ့နောက်ကိုက်ညီမှုရှိစေရန်အတွက် ဤစာတမ်းတစ်လျှောက်လုံး တွင် ဒစ်ဂျစ်တယ်လုံခြုံရေးဟူသော ဝေါဟာရကိုသာ အသုံးပြုထားသည်။ ၎င်းနယ်ပယ်တွင် ဤလမ်းညွှန်သည် အထူးသဖြင့် စောင့်ကြည့်မှု၊ ဖိနှိပ်မှုနှင့် အကြမ်းဖက်မှုတို့၏

[1] International Telecommunication Union, *Data Networks, Open System Communications and Security – Telecommunication Security, (International Telecommunications Union, 2008)* 2, https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.1205-200804-I!!PDF-E&type=items

ပစ်မှတ်ထားခြင်းခံရသည့် လူပုဂ္ဂိုလ်များနှင့် လူမှုအသိုင်းအဝိုင်းများ၏ ဘေးကင်းလုံခြုံမှု၊ လုပ်ပိုင်ခွင့် နှင့် အခွင့်အရေးများကို ဦးစားပေးထားသည်။

ဤလမ်းညွှန်သည် နိုင်ငံရေးအရမျက်ကွယ်ပြုထားသော သို့မဟုတ် ကြားနေသော အရာမဟုတ်ပါ။ နည်းပညာသည် လေဟာနယ်တွင် တည်ရှိနေခြင်းမဟုတ်ဘဲ အာဏာဖွဲ့စည်းပုံများအတွင်း ထည့်သွင်းထားသည် ဟူသော နားလည်မှုအပေါ် အခြေခံကာ ဤလမ်းညွှန်သည် ရည်ရွယ်ချက်ရှိရှိ ဆန့်ကျင်တွန်းလှန်ထားသော အရာဖြစ်သည်။ ဘက်မလိုက်၊ ကြားနေသည့် အသုံးအနှုံးများသည် ပိုနေမြဲကျားနေမြဲအခြေအနေကိုသာ ထိန်းသိမ်းရန် အထောက်အကူပြုစေသည်။ ဖိနှိပ်မှုနှင့် ကမ္ဘာလုံးဆိုင်ရာ ဖက်ဆစ်ဝါဒ၏ ခြိမ်းခြောက်မှုများကိုရင်ဆိုင်ရာတွင် ကြားနေခြင်းသည် လုံခြုံရေး/မှုကို နိုင်ငံရေးအရမျက်ကွယ်ပြုထားစေပြီး၊ အကြီးမားဆုံးသော အန္တရာယ်အချို့သည် ရာဇဝတ်ကောင်များထံမှ မဟုတ်ဘဲ စောင့်ကြည့်ပြီး၊ အမြတ်ထုတ်ဖိနှိပ်ရန် စွမ်းရည်နှင့် လှုံ့ဆော်မှုများရှိသည့် အစိုးရများနှင့် ကော်ပိုရေးရှင်းများ ကိုယ်တိုင်ထံမှ လာခြင်းဖြစ်သည် ဟူသောအချက်ကို ဖုံးကွယ်ထားစေပါသည်။

ဤလမ်းညွှန်တွင် ဖော်ပြထားသော ကိရိယာတွေဟာ ဒစ်ဂျစ်တယ်ဆိုင်ရာ မိမိကိုယ်တိုင်ကာကွယ်ရေးအတွက် အသုံးဝင်တဲ့၊ မှတ်တမ်းများအရ ၎င်းတို့၏ စွမ်းဆောင်ရည်များနှင့် သက်ဆိုင်မှုအပေါ် အခြေခံ၍ ထည့်သွင်းထားခြင်း ဖြစ်သည်။ ၎င်းကိရိယာအများစုကို Privacy Guides ၊ PrivacyTools.io ကဲ့သို့သော လူထုအခြေပြု အသိုင်းအဝိုင်းမှ ဦးဆောင်သည့် အရင်းအမြစ်များတွင် တွေ့ရသော နှိုင်းယှဉ်ချက်များနှင့် အကဲဖြတ်ချက်များ၊ လုံခြုံရေးဆိုင်ရာလုပ်ငန်း များတွင် တက်ကြွစွာ ပါဝင်နေသူများမှ ထိန်းသိမ်းထားသော မှတ်တမ်းများမှတစ်ဆင့် ရွေးချယ် ထား ခြင်းဖြစ်သည်[2]။ ဖော်ပြထားသော ကိရိယာတိုင်းနှင့် ကျွန်ုပ်တို့ ကိုယ်တိုင်အတွေ့အကြုံရှိသည်ဟု မဆိုလိုပါ၊ မည်သည့် ကိုးကားချက်ကိုမဆို ကျွန်ုပ်တို့၏ မူရင်းဆန်းစစ်ချက် ရလာဒ် အဖြစ် မယူဆသင့်ပါ ။ ကျွန်ုပ်တို့၏ ရွေးချယ်မှုများသည် ဤကိရိယာများကို နက်နက်နဲနဲ စမ်းသပ်၊ နှိုင်းယှဉ်၊ မှတ်တမ်းတင်ထားသော အခြားသူများ၊ သုတေသီများ၊ နည်းပညာရှင်များနှင့် အသိုင်းအဝိုင်းများ၏ လုပ်ဆောင်မှုများ အပေါ် အခြေခံထားပါသည်။ ဤစာတမ်းသည် သုတေသနပြုချက်များ၊ ကိုယ်တွေ့ဖြစ်ရပ်များနှင့် ကိုယ်တိုင် ရင်ဆိုင်ခဲ့ရသော အတွေ့အကြုံများ ကို မျှဝေခဲ့ကြသည့် ကိုယ်ရေးကိုယ်တာ လုံခြုံမှု ဆိုင်ရာ အကြံပေးပုဂ္ဂိုလ်များ၊ နည်းပညာရှင်များ နှင့် လူမှုအဖွဲ့ အစည်းများထံမှ ရရှိထားသည့် အချက်အလက်များကို စုစည်းဖော်ပြထားခြင်း ဖြစ်ပါသည်။ ကျွန်ုပ်တို့သည် အသစ်အဆန်းတစ်ခုကို တီထွင်နေခြင်းမဟုတ်ပါ။ ကျွန်ုပ်တို့သည် အထူးသဖြင့် အင်္ဂလိပ်ဘာသာစကားထက် ကျော်လွန်၍ ၎င်းကို လိုအပ်နေသူများအတွက် ပိုမိုအသုံး ပြုရလွယ်ကူစေရန် ရှိပြီးသားအရာများကို စနစ်တကျ စုစည်းပေးနေခြင်းသာ ဖြစ်သည်။

[2] "The collaborative privacy advocacy community," Privacy Guides, accessed April 20, 2025, https://www.privacyguides.org/en/; "Privacy Tools Guide: Website for Encrypted Software & Apps," Privacy Tools, https://www.privacytools.io/; eylenburg, "Sitemap - Eylenburg.github.io," *Eylenburg.github.io* (blog), accessed June 15, 2025, https://eylenburg.github.io/os_comparison.htm.

ကိုယ်ရေးကိုယ်တာလုံခြုံမှု (privacy)၊ လုံခြုံမှု(security) နှင့် အမည်မဖော်လိုခြင်း (anonymity)

ယခင်အပိုင်းတွင် ဤလမ်းညွှန်သည် ဝေါဟာရများနှင့်ပတ်သက်၍ ငြင်းခုံခြင်းမဟုတ်ကြောင်း ကျွန်ုပ်တို့ ဖော်ပြခဲ့ပါသည်။ ဒါပေမယ့် မဆိုင်းခဏပင် ဒီအခွင့်အရေး ရတာနဲ့ ချက်ချင်းဆိုသလိုကျွန်တော်တို့ ကိုယ့်စကားနဲ့ကိုယ် ပြန်ပြီး ဆန့်ကျင်နေမိပြန်ပါသည်။ သို့သော်လည်း၊ ဤအပိုင်းတွင် ကျွန်ုပ်တို့ ဆွေးနွေးမည့် ဝေါဟာရများသည် ဆိုက်ဘာ၊ သတင်း အချက်အလက်လုံခြုံရေးနှင့် ဒစ်ဂျစ်တယ်လုံခြုံရေးတို့၏ ဆိုင်ရာ ဘာသာစကားများနှင့် မတူညီကွဲပြားသော ကဏ္ဍတွင် တည်ရှိနေပါသည်။ အထူးသဖြင့် ကိုယ်ရေးကိုယ်တာလုံခြုံမှု (privacy)၊ လုံခြုံရေး (security) နှင့် အမည်မဖော်လိုခြင်း (anonymity) ဟူသည့် စကားလုံးများကို မတူညီသော အကြောင်းအရာများတွင် အပြန်အလှန် အသုံးပြုလေ့ရှိရာ၊ ၎င်းသည် ရှုပ်ထွေးမှုများ ဖြစ်စေပြီး လုံခြုံသည်ဟူသော မှားယွင်းသည့် ခံစားချက်ကို ဖန်တီးပေးနိုင်စေသောကြောင့် ဖြစ်ပါသည်။

ဥပမာအားဖြင့်၊ ကိုယ်ပိုင်ကွန်ရက်အတု (Virtual Private Networks(VPN)) ကို ကြည့်ပါ။ ကိုယ်ပိုင်ကွန်ရက်အတု (VPN) ကုမ္ပဏီများသည် ကိုယ်ပိုင်ကွန်ရက်အတု (VPN) သည် သင့်ကို အမည်မဖော်လိုသူဖြစ်စေသည်ဟု မကြာခဏဆိုသလို ကြော်ငြာကြသည်။ ၎င်းအချက်သည် ဤလမ်းညွှန်တွင် ကျွန်ုပ်တို့ ချေဖျက်လိုသည့် ပထမဆုံးသော အယူအဆများဖြစ်သည်။ ကိုယ်ပိုင်ကွန်ရက်အတု (VPN) များသည် ဆင်ဆာဖြတ်တောက်မှုနှင့် တည်နေရာကန့်သတ် ချက်များကို ကျော်လွှားခြင်း ကဲ့သို့သော သီးခြားခြိမ်းခြောက်မှုပုံစံများတွင် အသုံးဝင်သော်လည်း၊ ၎င်းတို့ကို လုံးဝအမည် မဖော်လိုသူဖြစ်စေသည်ဟု ခွဲခြားချက်မရှိ မယူဆသင့်ပါ။

ကိုယ်ပိုင်ကွန်ရက်အတု (VPN) တစ်ခုသည် ဝန်ဆောင်မှုပေးသူ၏ ဆာဗာနှင့် သင့်စက်ပစ္စည်းအကြား စာဝှက်ထားသော လမ်းကြောင်းတစ်ခုကို ဖန်တီးပေးသည်။ ၎င်းအချက် သည် သင့်၏ ဒိုမိန်း (Domain) အမည်များကို အိုင်ပီလိပ်စာ (IP) အဖြစ် ပြောင်းလဲပေးသည့်စနစ် (DNS) တောင်းဆိုမှုများ သည်ပင် ထိုလမ်းကြောင်းမှတစ်ဆင့် လုံခြုံစွာ သွားလာနိုင်ကြောင်းကို ပြသသည်။ သင့်စက်ပစ္စည်းများက ကိုယ်ပိုင်ကွန်ရက်အတု (VPN) ကို အသုံးပြုသည့်အခါ၊ သင့်စက်ပစ္စည်းများသည် ကိုယ်ပိုင်ကွန်ရက်အတု (VPN) ၏ ဒေသတွင်း ကွန်ရက်၏ အစိတ်အပိုင်းတစ်ခု ဖြစ်လာသည်။ ဤအကြောင်းကြောင့်၊ သင့်အင်တာနက် အသွား အလာသည် သင့်၏ အိုင်ပီလိပ်စာ (IP) အစစ်မှ လာခြင်းမဟုတ်ဘဲ ကိုယ်ပိုင်ကွန်ရက်အတု (VPN) ဆာဗာ၏ အိုင်ပီလိပ်စာ (IP) မှ လာနေပုံပေါက်မည်ဖြစ်သည်။ ထို့ကြောင့် ကိုယ်ပိုင်ကွန်ရက်အတု (VPN) သည် သင့်၏ လက်ရှိတည်နေရာကို ဖုံးကွယ်ပေးပြီး အင်တာနက်အသွားအလာကို အင်တာနက်ဝန်ဆောင်မှုပေးသူ (ISP) က မြင်တွေ့ခြင်းမှ ကာကွယ်ပေးသည်။ အင်တာနက်ဝန်ဆောင်မှုပေးသူ (ISP) မည်သူ ဖြစ်သည်က ို သင်မသိပါက www.dnschecker.org/what-is-my-isp.php သို့ ဝင်ရောက်ခြင်းဖြင့် အလွယ်တကူ ရှာဖွေနိုင်ပါသည်။

ကိုယ်ပိုင်ကွန်ရက်အတု (VPN) နှင့် ချိတ်ဆက်ခြင်းသည် သင့်အင်တာနက်အသွားအလာကို သင့် အင်တာနက် ဝန်ဆောင် မှုပေးသူ (ISP) မှ ဖုံးကွယ်ထားသော်လည်း သင့်ကို အမည်မဖော်လိုသူဖြစ်အောင် လုပ်ဆောင် မပေး နိုင်ပါ။ သင့် အင်တာနက်ဝန်ဆောင်မှုပေးသူ (ISP) က သင်သည် ကိုယ်ပိုင်ကွန်ရက်အတု (VPN) နှင့် ချိတ်ဆက် အသုံးပြု ထားကြောင်းကို သိပါသည်။ ထို့ကြောင့် ကိုယ်ပိုင်ကွန်ရက်အတု (VPN) ဝန်ဆောင်မှုပေးသူများသည် သင့်အတွက် ကြားခံလူအသစ်ဖြစ်လာပြီး သင်သည် သင်၏ယုံကြည်စိတ်ချမှုကို အဖွဲ့အစည်းတစ်ခုမှ အခြား တစ်ခုသို့ ပြောင်းရွှေ့လိုက် ခြင်းပင် ဖြစ်သည်။

ကိုယ်ပိုင်ကွန်ရက်အတု (VPN) ဝန်ဆောင်မှုပေးသူများသည် သင့်၏ အိုင်ပီလိပ်စာ (IP) အစစ်၊ ရုပ်ပိုင်းဆိုင်ရာ တည်နေရာနှင့် ချိတ်ဆက်မှုဆိုင်ရာ အချိန်မှတ်တမ်း (timestamps) ကဲ့သို့သော အချက်အလက်များကို ရယူနိုင် ပါသည်။ ကိုယ်ပိုင်ကွန်ရက်အတု (VPN) သည် သင့်အင်တာနက်အသွားအလာကို အင်တာနက်ဝန်ဆောင်မှုပေးသူ (ISP) မှ ဖုံးကွယ်ပေးပြီး ပထဝီဝင်ဆိုင်ရာ ကန့်သတ်ချက်များကို ကျော်လွှားနိုင်စေသော်လည်း ၎င်းသည် မှော် ဆန်သည့်အရာ မဟုတ်သည့်အတွက် ၎င်း၏ကန့်သတ်ချက်များကို ရှင်းလင်းစွာ နားလည်ပြီး သတိဖြင့် အသုံးပြု သင့်ပါသည်။

ကျွန်ုပ်တို့၏ အဓိကထားဆွေးနွေးလိုတဲ့အကြောင်းအရာဖြစ်သည့် ကိုယ်ရေးကိုယ်တာလုံခြုံမှု (Privacy)၊ လုံခြုံမှု (Security) နှင့် အမည်မဖော်လိုခြင်း (Anonymity) တို့၏ ကွာခြားချက်ကို ပြန်လည်ဆွေးနွေးကြပါစို့။ ကိုယ်ရေး ကိုယ်တာလုံခြုံမှု (Privacy) ဆိုသည်မှာ သင့်အချက်အလက်များကို မည်သူက ရယူခွင့်ရှိသည်ကို ထိန်းချုပ်ခြင်း ဖြစ်သည်[3]။ ကိုယ်ရေးကိုယ်တာလုံခြုံမှု (Privacy) ဆိုသည်မှ မည်သည့်အရာကို မည်သူနှင့် မျှဝေရမည်ကို သင် ကိုယ်တိုင် ရွေးချယ်ဆုံးဖြတ်ခြင်းနှင့် သက်ဆိုင် သည်။ တစ်ဖက်တွင် လုံခြုံရေး (Security) ဆိုသည်မှာ သင့် အချက် အလက်များကို ဘေးကင်းလုံခြုံစေရန်အတွက် သင်ပြု လုပ်သော လုပ်ဆောင်မှုများကို ဆိုလိုခြင်းဖြစ်ပါ တယ်။ နောက်ဆုံးအနေ နဲ့ အမည်မဖော်လိုခြင်း (Anonymity) ဆိုသည်မှာ သင့်၏ မည်သူမည်ဝါဖြစ်မှုကို ထုတ်ဖော်ခြင်းမရှိဘဲ သင့်ကိုယ်သင် ဖော်ပြနိုင်ခြင်းကို ခွင့်ပြုခြင်းဖြစ်သည်။ ဤအယူအဆများသည် တစ်ခုနှင့် တစ်ခု အတူယှဉ်တွဲ တည်ရှိနိုင်သော်လည်း ၎င်းတို့သည် တစ်ခုနှင့်တစ်ခု သီးခြားရပ်တည်နေသော အရာများ မဟုတ်ပေ။ လုံခြုံမှု (Security) မရှိဘဲ ကိုယ်ရေးကိုယ်တာလုံခြုံမှု (Privacy) ရှိနိုင်သည်။ ကိုယ်ပိုင်မှတ်စုစာအုပ် တစ်အုပ်တွင် သင့်အတွေးများကို ချရေးနေပါက၊ သင့်အတွေးများကို သင့်ဘာသာသိမ်းထားရန် သင်ကိုယ်တိုင် ရွေးချယ်နိုင်သည့် ကိုယ်ပိုင်နေရာတစ်ခု ရှိနေခြင်းဖြစ်သည်။ ကိုယ်ရေးကိုယ်တာလုံခြုံမှုဆိုသည်မှာ ထိုသို့ပင် ဖြစ်သည်။ သင်၏အချက်အလက်များကို မည်သူရယူနိုင်သည်ကို ထိန်းချုပ်နိုင်ခြင်းသည် ကိုယ်ရေးကိုယ်တာ လုံခြုံမှု၏ အဓိကအချက်ဖြစ်သည်။ သို့သော် ထိုမှတ်စုစာအုပ်တွင် သော့ခတ်ထားခြင်းမရှိခြင်း သို့မဟုတ် လုံခြုံ သောနေရာတွင် မထားရှိခြင်းတို့ကြောင့် မည်သူမဆို ရည်ရွယ်ချက်ရှိသည် ဖြစ်စေ၊ မရှိသည်ဖြစ်စေ ထိုမှတ်စုစာ အုပ်ကို မတော်တဆတွေ့ရှိပြီး သင်၏ကိုယ်ပိုင်အတွေး များကို ဖတ်ရှုသွားနိုင်သည်။ ဤအခြေအနေ၏ ဆန့်ကျင်ဘက်ဖြစ်သည့် ကိုယ်ရေးကိုယ်တာလုံခြုံမှု (Privacy) မရှိဘဲ လုံခြုံမှုရှိခြင်း (Security) ကို သင့်လုပ်ငန်း

[3] Derek E. Bambauer, "Privacy Versus Security," *Journal of Criminal Law and Criminology 103*, no. 3 (2013): 667-684

သုံး စက်ပစ္စည်းဖြစ်သည့် ကွန်ပျူတာ၊ ဖုန်း အစရှိသည်ကို အသုံးပြုခြင်းဖြင့် မြင်သာစေသည်။ သင့်အလုပ်နေရာသည် ဆိုက်ဘာတိုက်ခိုက်မှုများမှ ကွန်ရက်ကို ကာကွယ်ရန် ခိုင်မာသော လုံခြုံရေးအစီအမံများကို အကောင်အထည်ဖော်ထားနိုင်သည်။ သို့သော်လည်း ဤလုံခြုံရေးစည်းမျဉ်းများတွင် ဝန်ထမ်းများ၏ အီးမေးလ် အကောင့်များနှင့် အွန်လိုင်းလှုပ်ရှားမှုများကို ခြေရာခံခြင်းတို့ ပါဝင်နိုင်သဖြင့် ၎င်းတို့၏ ဆက်သွယ်မှုများတွင် ကိုယ်ရေးကိုယ်တာလုံခြုံမှု (Privacy) အကြီးအကျယ် ဆုံးရှုံးစေနိုင်သည်။

နောက်ဆုံးအနေဖြင့်၊ အမည်မဖော်လိုခြင်း (Anonymity) ဆိုသည်မှာ သင့်၏ မည်သူမည်ဝါဖြစ်မှုကို မသိရှိစေခြင်း သို့မဟုတ် ထုတ်ဖော်ခြင်းမပြုခြင်းဖြစ်သည်။ အမည်မဖော်လိုခြင်း (Anonymity) ကို ကိုယ်ရေးကိုယ်တာလုံခြုံမှု (Privacy) နှင့် မကြာခဏ မှားယွင်းတတ်သော်လည်း ၎င်းတို့သည် အလွန်ကွာခြားသည့် အယူအဆနှစ်ခုဖြစ်သည်။ ကိုယ်ရေးကိုယ်တာလုံခြုံမှု (Privacy) ကို သင့်ပြတင်းပေါက်တွင် အလင်းမဖောက်နိုင်သော လိုက်ကာများ တပ်ဆင်ထား ခြင်းနှင့် နှိုင်းယှဉ်ဖော်ပြ နိုင်ပြီး၊ အမည်မဖော်လိုခြင်း (Anonymity) မှာမူ မျက်နှာကို ဖုံးကွယ်ထားသည့် မျက်နှာဖုံးတစ်ခု ဝတ်ဆင် ထားခြင်းနှင့် တူညီပါသည်။ တစ်စုံတစ်ဦးသည် ကလောင်အမည်ဖြင့်ဖြစ်စေ၊ အခြားနည်းလမ်းဖြင့်ဖြစ်စေ အမည်မဖော်ဘ ` (Anonymous) ရှိနေသောအခါ၊ ၎င်းတို့၏ လုပ်ဆောင်မှုများ သို့မဟုတ် ဆက်သွယ်မှုပြောဆိုမှုများကို ၎င်းတို့ထံ ပြန်လည်ခြေရာခံ ၍မရနိုင်ပေ။ အင်တာနက်ကွန်ရက်များအသုံးပြုနေစဉ် အမည်မဖော်လိုသူအဖြစ် ရှိနေရန်မှာ ခက်ခဲပြီး၊ မိမိမည်သူမည်ဝါ ဖြစ်ကြောင်း ဆုံးဖြတ်ပေးနိုင်သော ကိုယ်ပိုင် အချက်အလက်အမှန်များ နှင့် မိမိ၏လုပ်ဆောင်မှုများကို ခြေရာခံခြင်းနှင့် စောင့်ကြည့် ခြင်းတို့မှ လျှို့ဝှက်ထားရန်အတွက် ရှုပ်ထွေးသော လုပ်ငန်းစဉ်များ လိုအပ်သည်။ အမည်မဖော်လိုခြင်း (anonymity) သည် ပြီးခဲ့သည့် ဆယ်စုနှစ်ခန့်အတွင်း ဒစ်ဂျစ်တယ်လုံခြုံရေးနယ်ပယ်တွင် ပြင်းပြင်းထန်ထန် ငြင်းခုံဆွေးနွေးခဲ့ကြသည့် အကြောင်းအရာများထဲမှ တစ်ခုဖြစ်သည်။ Electronic Frontiers Foundation (EFF) အတွက် ရေးသားခဲ့သည့် ဆောင်းပါတွင် စာရေးသူ York က အမည်မဖော်လို (anonymity) ခွင့်ကို ထိန်းသိမ်းခြင်းသည် လွတ်လပ်စွာ ထုတ်ဖော်ပြောဆိုခွင့်နှင့် လုံခြုံရေးအတွက် မရှိမဖြစ်လိုအပ်ကြောင်း အခိုင်အမာ ဆိုထားသည်[4]။ ကမ္ဘာကြီးသည် နိုင်ငံရေးအရ ပိုမိုပြီး ဆန်ကျင့်သော အစွန်းနှစ်ရပ်ကိုရောက်လာသည်နှင့်အမျှ ဤအချက်သည် ယခင်ကထက် ယခုအချိန်တွင် ပိုမိုအရေးကြီးလာသည်။ Electronic Frontiers Foundation (EFF) ကလည်း အမည်မဖော်ဘဲ ပြောဆိုခြင်းသည် အာဏာပိုင်များကို တာဝန်ခံမှုရှိစေရန်၊ အာဏာအလွဲသုံးစားလုပ်မှုများကို ဖော်ထုတ်ရန်နှင့် နိုင်ငံရေးအဂတိလိုက်စားမှု သို့မဟုတ် ပြည်သူ့ကျန်းမာရေးအကျပ်အတည်းများကဲ့သို့သော ပြဿနာများ၏ အမှန်တကယ်ဆိုးရွားမှုကို ဖော်ထုတ်ရန်အတွက် အရေးပါသောအခန်းကဏ္ဍမှ ပါဝင်သည်ဟု ထောက်ပြထားပါသည်။

အခြေအနေတစ်ခုကို ဖော်ပြဖို့အတွက် မှန်ကန်တဲ့ ဝေါဟာရကို ရွေးချယ်နိုင်ခြင်းက အဲဒီအခြေအနေကို ပိုပြီး ကောင်းမွန် စွာ နားလည်အောင် ကူညီပေးနိုင်ပါတယ်။ ဒါ့အပြင် အန္တရာယ်ခြိမ်းခြောက်မှုဆိုင်ရာ ပုံစံ (threat

[4] Jillian C. York, "The right to anonymity is vital to free expression: now and always," *Electronic Frontier Foundation*, March 25, 2020. https://www.eff.org/deeplinks/2020/03/right-anonymity-vital-free-expression-now-and-always

model) အကြောင်း ဆွေးနွေးတဲ့အခါမှာလည်း ဒီအချက်ဟာ အရေးကြီးတဲ့ အခန်းကဏ္ဍကနေ ပါဝင်မှာဖြစ်ပါတယ်။ တစ်ချို့လူ တွေအတွက်တော့ ကိုယ်ရေးကိုယ်တာလုံခြုံမှု (privacy)၊ အမည်မဖော်လိုခြင်း (anonymity) နဲ့ လုံခြုံရေး (security) စတဲ့အကြောင်းအရာတွေကို စာပိုဒ်ရှစ်ခုလောက် အချိန်ယူပြီး ပြောဆိုနေတာက အကျိုးမရှိဘူးလို့ ထင်ရနိုင်ပါတယ်။ ဒါပေမဲ့ ဒီအခြေခံအချက်တွေကို အစောပိုင်းကတည်းက တင်ပြထားဖို့က မရှိမဖြစ်လိုအပ်ပါတယ်။ ဒီလိုလုပ်ခြင်းအားဖြင့် ကျွန်တော်တို့ရဲ့ ဒစ်ဂျစ်တယ်ကမ္ဘာရဲ့ ရှုပ်ထွေးမှုတွေကို ပိုမိုကောင်းမွန်စွာ နားလည်လာနိုင်မှာ ဖြစ်ပါတယ်။

စာဝှက်လျှို့ဝှက်ကုဒ်စနစ်ကို ရှင်းလင်းနားလည်အောင် လုပ်ဆောင်ခြင်း (Demystifying encryption)

Five Eyes လို့ခေါ်တဲ့ နိုင်ငံတွေ (အမေရိကန်၊ ယူကေ၊ ကနေဒါ၊ ဩစတြေးလျ နဲ့ နယူးဇီလန်) အပါအဝင် ကမ္ဘာတစ်ဝန်းက အစိုးရအဖွဲ့အစည်းများစွာဟာ စာဝှက်လျှို့ဝှက်ကုဒ်စနစ် (encryption) ကို အပြင်းအထန် ဆန့်ကျင်တိုက်ဖျက်ဖို့ ကြိုးပမ်းလာတာကြောင့် စာဝှက်လျှို့ဝှက်ကုဒ်စနစ် (encryption) ရဲ့ပုံစံက ဘယ်လို ဖြစ်သင့်လဲဆိုတဲ့အပေါ် အချေအတင် ငြင်းခုံမှုတွေ ပိုပြီး ပြင်းထန်လာပါတယ်[5]။ ပိုပြီး တိတိကျကျပြောရရင် ဒီအငြင်းပွားမှုဟာ စာဝှက်လျှို့ဝှက်ကုဒ်စနစ် (encryption) က တစ်ဦးချင်းစီရဲ့ ကိုယ်ရေးကိုယ်တာ လုံခြုံမှုကို ကာကွယ်ပေးနိုင်တဲ့ အခန်းကဏ္ဍ နဲ့ ရာဇဝတ်မှု တားဆီးနိုင်ရန်အတွက် ဒီစနစ်များအတွင်း ဝင်ရောက်စစ်ဆေးခွင့်ပေးထား ရန် လိုအပ်ခြင်း ဆိုတဲ့ အချက်တွေကြားက ပဋိပက္ခတစ်ခုဖြစ်လာ ပါတယ်။ Alliance for Citizen Engagement အဖွဲ့အစည်းက စာဝှက်လျှို့ဝှက်ကုဒ်စနစ် များအတွင်း ဝင်ရောက်စစ်ဆေးခွင့် ပေးထားခြင်း (encryption backdoor) ကို "ခွင့်ပြုချက် ရှိသည်ဖြစ်စေ၊ မရှိသည်ဖြစ်စေ မည်သည့်နည်းလမ်းနဲ့မဆို စာဝှက်လျှို့ဝှက်ကုဒ်စနစ် (encryption) ကို ကျော်ဖြတ်၍ အချက်အလက်များကို တစ်စုံတစ်ယောက်ကို ရယူစေနိုင်ခြင်း" ဟု အဓိပ္ပာယ်ဖွင့်ဆိုထာပါသည်[6]။ စာဝှက်လျှို့ဝှက်ကုဒ် စနစ် များအတွင်း ဝင်ရောက်စစ်ဆေးခွင့်တွေ ဖန်တီးဖို့ လိုလားသူတွေရဲ့ အကြောင်းပြချက်ကတော့ ဆိုးဝါးပြင်းထန်တဲ့ ရာဇဝတ်မှုတွေကို စုံစမ်းစစ်ဆေးဖို့အတွက် ဥပဒေစိုးမိုးရေး နဲ့ ထောက်လှမ်းရေး အေဂျင်စီတွေဟာ ကုဒ်ဝှက်ထားတဲ့ ဆက်သွယ်မှုတွေကို ဝင်ရောက်ကြည့်ရှုခွင့် လိုအပ်ပါတယ်ဆိုတဲ့အချက်ပဲ ဖြစ်ပါတယ်။ အမေရိကန်ပြည်ထောင်စုရဲ့ ဗဟိုပြည်ထောင်စုစုံစမ်းစစ်ဆေးရေးဗျူရို (FBI) က သူတို့အတွက် စာဝှက်လျှို့ဝှက်ကုဒ်စနစ် အတွင်း ဝင်ရောက်စစ်ဆေးခွင့် လုပ်ဆောင်ချက်ဟာ လိုအပ်ပြီး တရားမျှတတယ်လို့ ပုံဖော်ဖို့အတွက် အဲဒီဝေါဟာရကို တာဝန်ယူမှုရှိစွာ စီမံခန့်ခွဲထားသော စာဝှက်လျှို့ဝှက်ကုဒ်စနစ် (responsibly managed encryption) လို့ နာမည်ပြောင်းလဲခဲ့ပါတယ်[7]။ သို့သော်လည်း အရပ်ဘက်လူ့အဖွဲ့အစည်းများနဲ့ ကိုယ်ရေးကိုယ်တာလုံခြုံမှုကို အလေးပေး လိုလားသူများကတော့ စာဝှက်

[5] Mallory Knodel et al., "Five Eyes campaign against encryption threatens democracy," *Tech Policy Press*, October 11, 2023, https://www.techpolicy.press/five-eyes-campaign-against-encryption-threatens-democracy/

[6] Michael Akoto, "Understanding the investigatory encryption backdoor debate," *The Alliance for Citizen Engagement*, January 26 2025, https://ace-usa.org/blog/research/research-technology/understanding-the-investigatory-encryption-backdoors-debate/

လျှို့ဝှက်ကုဒ်စနစ် များ အတွင်း ဝင်ရောက်စစ်ဆေးခွင့် ဖန်းတီးထားခြင်းသည် လူတိုင်းရဲ့ စာဝှက်လျှို့ဝှက်ကုဒ်စနစ် (encryption) စနစ်ကို အားနည်းစေတယ်လို့ ဆိုကြပါတယ်။ ကောင်းတဲ့လူတွေအတွက်ပဲ ဖန်တီးထားတဲ့ စာဝှက်လျှို့ဝှက်ကုဒ်စနစ်များအတွင်းဝင်ရောက်စစ်ဆေးခွင့် မရှိပါဘူး[8]။ ပစ္စုပ္ပန်အချိန်အခါမှာ အမြင်မတူသဘောထား ကွဲမှု၊ ကန့်ကွက်ဆန္ဒပြမှု ပုံစံအားလုံးကို နှိမ်နင်းပြီး ထိန်းချုပ်နေတဲ့အတွက် ဘယ်သူက လူကောင်းလဲဆို တာကို ခွဲခြားဖို့ ပိုပြီးခက်ခဲလာပါတယ်။ (တကယ်လို့ လူကောင်းဆိုတာ ရှိခဲ့ရင်ပေါ့)။ သူရဲ့ ဖွဲ့စည်းတည်ဆောက်ပုံသဘော တရားအရ ပြောရမယ်ဆိုရင် စာဝှက်လျှို့ဝှက်ကုဒ်စနစ်ဆိုတာ လူတိုင်းအတွက် လုံခြုံမှု ရှိရင်မရှိ ဒါမှမဟုတ် ဘယ်သူ့အတွက်မှ လုံခြုံမှုမရှိတာ နှစ်မျိုးပဲ ရှိပါတယ်။

စာဝှက်လျှို့ဝှက်ကုဒ်စနစ် (Encryption) ဟာ အင်တာနက်ပေါ်က ကိုယ်ရေး ကိုယ်တာလုံခြုံမှုရဲ့ အဓိကကျောရိုးဖြစ်ပါတယ်[9]။ Global Encryption Coalition က ထုတ်ပြန်တဲ့ သတင်းတစ်ရပ်မှာ သတင်းပေးဖော် ကောင်လုပ်ခဲ့သူ အက်ဝါ့ဒ် စနိုးဒင် (Edward Snowden) က သူ့ရဲ့အတွေ့အကြုံအရ အစိုးရတွေကို စာဝှက်လျှို့ဝှက်ကုဒ်စနစ် (encryption) ကို ကျော်လွှားနိုင်တဲ့ ကိရိယာတွေ ပေးလိုက်တဲ့အခါ သူတို့ဟာ မူလရည်ရွယ်ချက်ကို ကျော်လွန်ပြီး အဲဒီအခွင့်အရေးကို မကြာခဏ အလွဲသုံးစားလုပ်လေ့ရှိတယ်လို့ သတိပေးပြောကြားခဲ့ပါတယ်[10]။ နိုင်ငံတော်လုံခြုံရေး အမည်ခံပြီး အာဏာပိုင်တွေဟာ အပြစ်မဲ့ပြည်သူတွေကို မည်သို့မည်ပုံ စောင့်ကြည့်ထောက်လှမ်းခဲ့တယ်၊ တာဝန် ယူမှုတာဝန်ခံမှုမရှိဘဲ ကိုယ်ရေးကိုယ်တာ အချက်အလက်တွေကို စုဆောင်းခဲ့တယ် ဆိုတာကို သူကိုယ်တိုင် တွေ့ကြုံခဲ့ ရဖူးတယ်လို့ ဆိုပါတယ်။ စနိုးဒင် (Snowden) ရဲ့အမြင်မှာတော့ စာဝှက်လျှို့ဝှက်ကုဒ်စနစ် များအတွင်း ဝင်ရောက်စစ် ဆေးခွင့် ဖန်တီးဖို့ စိတ်ကူးဟာ ဘဝပေါင်းများစွာကို အန္တရာယ်ဖြစ်စေပြီး အစုလိုက်အပြုံလိုက် စောင့်ကြည့် ထောက်လှမ်းမှုတွေအတွက် အိတ်သွင်ဖာမှောက်ဖွင့်ပေးသလိုမျိုး ဖြစ်စေနိုင်တဲ့ ပေါ့ဆတဲ့လုပ်ရပ်တစ်ခုပဲ ဖြစ်တယ်လို့ ဆိုပါတယ်။ စာဝှက်လျှို့ဝှက်ကုဒ်စနစ် (encryption) ဟာ အပေးအယူလုပ်ပြီး ဖြေလျှော့ပေး လိုက်ရပြီဆိုရင် သတင်းထောက်တွေ၊ လှုပ်ရှားတက်ကြွသူတွေ၊ သက်သေခံအချက်အလက် ဖော်ထုတ်တိုင်ကြားလိုသူတွေ၊ အိမ်တွင်းအကြမ်းဖက်မှု ခံရသူတွေန့ဲ့ သာမန်ပြည်သူတွေအတွက်ပါ အချက်အလက်ပေါက်ကြားမှု၊ ဆင်ဆာ ဖြတ်တောက်မှုန့ဲ့ ပိုပြီးကြီးမားတဲ့ ပြဿနာဖြစ်တဲ့ အစုလိုက်အပြုံလိုက် စောင့်ကြည့်ထောက်လှမ်းမှုတွေ ကနေကာကွယ် ပေးထားတဲ့ အကာအကွယ် အနည်းငယ်ကိုပါ ဆုံးရှုံးစေပါတယ်။

---

7 "Warrant-proof encryption and lawful access," Federal Bureau of Investigation, accessed April 10, 2025, https://www.fbi.gov/how-we-investigate/lawful-access

8 Joe Mullin and Cindy Cohn, "Salt Typhoon Hack Shows There's No Security Backdoor That's Only For The "Good Guys," *Electronic Frontiers Foundation*, October 9, 2024, https://www.eff.org/deeplinks/2024/10/salt-typhoon-hack-shows-theres-no-security-backdoor-thats-only-good-guys

9 Brittany Day, "The importance of strong encryption in digital privacy and security," Linux Security (blog), January 07, 2020, https://linuxsecurity.com/features/encryption-an-essential-yet-highly-controversial-component-of-digital-security

10 Global Encryption Coalition admin, "Edward Snowden and the Global Encryption Coalition say "Meddling with strong encryption puts public and economy at risk, " Global Encryption Coalition, published October 21, 2021, https://www.globalencryption.org/2021/10/edward-snowden-and-the-global-encryption-coalition-say-meddling-with-strong-encryption-puts-public-and-economy-at-risk-press-release/

အနှစ်ချုပ်ပြောရရင် စာဝှက်လျှို့ဝှက်ကုဒ်စနစ် (encryption) ဆိုတာ အချက် အလက်တွေကို ကုဒ်ဝှက်စာသား (ciphertext) အဖြစ် ပြောင်းလဲပေးတဲ့ နည်းလမ်းတစ်ခု ဖြစ်ပါတယ်။ ဒီနည်းလမ်းက သာမန်စာသား (plaintext) လို့ ခေါ်တဲ့ အချက်အလက်တွေကို မှန်ကန်တဲ့ ကုဒ်ဖြေသော့ (decryption key) မရှိတဲ့ မည်သူ့ကိုမဆို ဖတ်မရအောင် ပြုလုပ်ပေးပါတယ်။ အနှစ်သာရအားဖြင့် စာဝှက်လျှို့ဝှက်ကုဒ်စနစ် (encryption) ဟာ သော့ (key) တစ်ခုကို အသုံးပြုပြီး အလုပ်လုပ်ပါတယ်။ ဒီသော့က သာမန်စာသား(plaintext) ကို ဘယ်လို ကုဒ်ဝှက်ရမယ်၊ ကုဒ်ဘယ် လိုပြန်ဖြေရမယ်ဆိုတာကို ဆုံးဖြတ်ပေးပါတယ်။ ဥပမာအနေနဲ့ ပြောရရင် ဒီစာအုပ်ကို ရေးသားသူ တစ်ဦးဖြစ်တ ဲ့ ဂျင်းဒင်ကို (Jean Dinco) ဟာ မူလတန်းကျောင်းတက်စဉ်က တြိဂံရဲ့ ထောင့်မှန်ခံအနား (hypotenuse) အကြောင်း သင်ခန်းစာရာမ ပြောတာ ကို နားထောင်မယ့်အစား သူ့ဘေးနားက စာသင်ဖော်နဲ့ စကားပြောရင်း အချိန်ကုန်ဆုံးခဲ့ရပုံကို ကြည့်ပါ။ ကျိန်းသေပေါက် ဒါက ဆရာမ တီနာ (Tina) အတွက်တော့ စိတ်ပျက်စရာပါပဲ။ သူတို့ရဲ့ စကားဝိုင်းတွေကို လျှို့ဝှက်ထားနိုင်ဖို့အတွက် ဂျင်း (Jean) နဲ့ သူ့သူငယ်ချင်း ရော့ဇန် (Roxanne) တို့ဟာ သူတို့ကိုယ်ပိုင် အက္ခရာ တွေကို ဖန်တီးခဲ့ကြပါတယ်။ အချက်အလက်တွေကို လျှို့ဝှက်ကုဒ် အဖြစ် ပြောင်းလဲတဲ့စနစ် ရယ်၊ လျှို့ဝှက်သော့ ရဲ့ အကူအညီနဲ့ 'HELLO' ဆိုတဲ့ စကားလုံးဟာ 'KHOOR' ဆိုပြီး ဖြစ်သွားပါတယ်။ ရှင်းပါတယ်။ သူတို့နှစ်ယောက်စလုံးက ရိုးရှင်းတဲ့ ကုဒ်ဝှက်နည်းစနစ် (Ceasar cipher) ကို အသုံးပြုခဲ့ကြတာပါ။ ဒီစနစ်က အက္ခရာရဲ့တန်ဖိုးကို ရွှေ့ရုံပါပဲ[11]။ ဒီကိစ္စမှာတော့ အက္ခရာတွေကို သုံးလုံးရွှေ့ခဲ့ တာဖြစ်ပါတယ်။ 'H' ဟာ အက္ခရာစဉ်ရဲ့ ၈ လုံးမြောက်စာလုံးဖြစ်တဲ့အတွက် ၈+၃=၁၁ ဆိုတဲ့ ရိုးရှင်းတဲ့ ပေါင်း ခြင်းတွက်နည်းကို သုံးပြီး 'H' နေရာမှာ အစားထိုးရမယ့် စာလုံးက 'K' ဖြစ်တယ်ဆိုတာကို သိနိုင်ပါတယ်။ ဒါက ဆရာမအနေနဲ့ မိနစ်ပိုင်းအတွင်း ဖြေရှင်းနိုင်တဲ့ အားနည်းတဲ့ စာဝှက်လျှို့ဝှက်ကုဒ်စနစ် (encryption) နည်းလမ်း တစ်ခု ဖြစ်ပေမဲ့ ဒီအခြေခံသဘောတရားကို သရုပ်ဖော်ပြဖို့ အတွက်တော့ လုံလောက်ပါတယ်။

အလုံးစုံစာဝှက်လျှို့ဝှက်ကုဒ်စနစ် (E2E)

Signal ဒါမှမဟုတ် WhatsApp အပလီကေးရှင်းတွေ နဲ့ပတ်သက်တဲ့ အကြောင်းတွေကြားရတဲ့အခါ ကျွန်တော်တို့ဟာ အလုံးစုံစာဝှက်လျှို့ဝှက်ကုဒ်စနစ် (end-to-end encryption) ၊ သယ်ယူပို့ဆောင်နေစဉ် စာဝှက်လျှို့ဝှက်ကုဒ်စနစ် (transport encryption) နဲ့ အသုံးမပြုဘဲနားနေစဉ် စာဝှက်လျှို့ဝှက်ကုဒ်စနစ် (encryption at rest) စတဲ့ ဝေါဟာရတွေကို မကြာ ခဏ ကြားရလေ့ရှိပါတယ်။ ဒီစကားစုတွေကို ပေးထားတဲ့ဝန်ဆောင်မှုဟာ လုံခြုံကြောင်း သက်သေပြဖို့အတွက် အသုံးပြုကြပေမဲ့ လက်တွေ့မှာတော့ ဒီထက်ပိုပြီး နက်နဲရှုပ်ထွေးပါတယ်။ အလုံးစုံစာဝှက် လျှို့ဝှက်ကုဒ်စနစ် (End-to-end encryption-E2EE) ဆိုတာကတော့ စာပို့သူနဲ့ စာကိုလက်ခံရရှိသူ နှစ်ဦးတည်းသာ အဲဒီစာကို ဖတ်နိုင်တယ်လို့ အဓိပ္ပာယ်ရပါတယ်။ သင့်ရဲ့စက်ပစ္စည်း ပေါ်မှာရှိတဲ့ အချက်အလက်တွေကို လျှို့ဝှက်ကုဒ် အဖြစ်ပြောင်းလဲ လိုက်ပြီး လက်ခံရရှိသူရဲ့ စက်ပစ္စည်း ပေါ် ရောက်မှသာ

[11] Dennis Luciano and Gordon Prichett, "Cryptology: From Caesar ciphers to public-key cryptosystems," *The College Mathematics Journal 18*, no. 1 (1987): 2-17, https://www.tandfonline.com/doi/abs/10.1080/07468342.1987.11973000

ကုဒ်ပြန်ဖြေပေးတာ ဖြစ်ပါတယ်[12]။ ဒီလိုဖြစ်တဲ့အတွက် ကြားခံလူတစ်ဦးတစ်ယောက်မှ (စာပို့တဲ့အက်ပလီကေးရှင်း၊ ကွန်ရက်၊ သင့်ရဲ့အင်တာနက်ဝန် ဆောင်မှုပေးသူ ဒါမှမဟုတ် ဆာဗာ) သင့်ရဲ့စာတွေကို ဖတ်လို့မရနိုင်ပါဘူး။ အလုံးစုံစာဝှက်လျှို့ဝှက်ကုဒ်စနစ် (End-to-end encryption-E2EE) နယ်ပယ်မှာတော့ Signal အက်ပလီကေးရှင်း က ဦးဆောင်နေတဲ့သူ ဖြစ်ပါတယ်။ Signal ကို အသုံးပြုတဲ့အခါ စာတွေကို ကုဒ်ဖြေဖို့အတွက် အသုံးပြုတဲ့ သော့တွေဟာ သင့်ရဲ့စက်ပစ္စည်း ထဲမှာပဲ သိမ်းဆည်းထားတာ ဖြစ်ပါတယ်။ ဒါကြောင့် အစိုးရရဲ့ဖိအားပေးမှုတွေ ဒါမှမဟုတ် ဆိုက်ဘာတိုက်ခိုက်သူတွေရဲ့ ထိုးဖောက်ဝင်ရောက်မှုတွေ ရှိလာရင်တောင် Signal က သင့်ရဲ့ စာတွေကို ပေးအပ်နိုင်မှာမဟုတ်ပါဘူး။ ဘာလို့လဲဆိုတော့ သူတို့မှာ ကုဒ်ဝှက်တဲ့ သော့တွေကို ဝင်ရောက်ကြည့်ရှုခွင့် မရှိလို့ပါပဲ။

လျှို့ဝှက်သော့တစ်မျိုးတည်းသုံးသောနည်း (symmetric) နှင့် လျှို့ဝှက်သော့နှစ်မျိုးသုံးသောနည်း (asymmetric)

စာဝှက်လျှို့ဝှက်ကုဒ်စနစ် (Encryption) ပုံစံနှစ်မျိုးရှိပါတယ်။ အဲဒါတွေကတော့ လျှို့ဝှက်သော့တစ်မျိုးတည်းသုံးသောနည်း (symmetric) နဲ့ လျှို့ဝှက်သော့ နှစ်မျိုးသုံးသောနည်း (asymmetric) တို့ပဲ ဖြစ်ပါတယ်။ လျှို့ဝှက်သော့တစ်မျိုးတည်းသုံးသော စာဝှက်လျှို့ဝှက်ကုဒ်စနစ် (Symmetric encryption) ဟာ အချက် အလက် (သာမန်စာသား) ကို ကုဒ်ဝှက်ဖို့နဲ့ ကုဒ်ပြန်ဖြေဖို့အတွက် လျှို့ဝှက်သော့ (key) တစ်ခုတည်းကိုပဲ အသုံးပြုပါတယ်။ ဒီလျှို့ဝှက်သော့ ဟာ စကားဝှက်တစ်ခုလို (secrete password) အလုပ်လုပ်ပြီး သော့မရှိတဲ့ ဘယ်သူ့ကိုမဆို မူရင်းစာသားကို ဖတ်လို့မရဘဲ ရှုပ်ထွေးအောင် ပြုလုပ်ပေးပါတယ်[13]။ လျှို့ဝှက်သော့တစ်မျိုးတည်း သုံးသောနည်း (symmetrical) လို့ခေါ်ရတဲ့အကြောင်းရင်းကတော့ သော့ခတ်တဲ့ဘက်နဲ့ သော့ဖွင့်တဲ့ဘက် နှစ်ဖက်စလုံးမှာ တူညီတဲ့ လျှို့ဝှက်သော့ကို အသုံးပြုလို့ပါပဲ။ လျှို့ဝှက်သော့တစ်မျိုးတည်းသုံးသော စာဝှက်လျှို့ဝှက်ကုဒ်စနစ် (Symmetric encryption) ဟာ အချက်အလက် ပမာဏ အများအပြားကို ကုဒ်ဝှက်ဖို့ လိုအပ်တဲ့အခါ သုံးကြတာကို ပိုပြီးနှစ်သက် ကြပါတယ်။ ဘာလို့လဲဆိုတော့ဒီနည်း က ပိုမြန်ပြီး ကွန်ပျူတာစွမ်းအင်လည်း ပိုသက်သာစေလို့ ဖြစ်ပါတယ်[14]။ လျှို့ဝှက်သော့တစ်မျိုးတည်းသုံးသော စာဝှက်လျှို့ဝှက်ကုဒ်စနစ် (Symmetric encryption) ဥပမာတွေအနေနဲ့ အဆင့်မြင့် စာဝှက်လျှို့ဝှက်ကုဒ်စနစ် (AES- Advanced Encryption Standard) နဲ့ အချက်အလက် စာဝှက်လျှို့ဝှက်ကုဒ်စနစ် (DES- Data Encryption Standard) တို့ ပါဝင်ပါတယ်။ ဒီနှစ်ခုထဲမှာတော့ အဆင့်မြင့် စာဝှက်လျှို့ဝှက်ကုဒ်စနစ် (AES) ဟာ မတူညီတဲ့ သော့အရွယ်အစားတွေ (၁၂၈၊ ၁၉၂၊ ၂၅၆) ကို ခွင့်ပြုပေးတဲ့အတွက် အများစုက ပိုပြီးနှစ်သက်ကြပါတယ်[15]။ အဆင့်မြင့် စာဝှက်

---

12 Randy Battat, "End-to-End Encryption: What it is & How it Works," *Preveil*, August 30, 2024, https://www.preveil.com/blog/end-to-end-encryption/.

13 Annie Badman and Matthew Kosinski, "What is symmetric encryption?," *IBM*, August 5, 2024, https://www.ibm.com/think/topics/symmetric-encryption.

14 Nicolas Poggi, "Encryption choices: RSA vs. AES explained," Prey Project (blog), June 2, 2025, https://preyproject.com/blog/types-of-encryption-symmetric-or-asymmetric-rsa-or-aes.

15 Joan Daemen and Vincent Rijmen, *The Design of Rijndael: AES — The Advanced Encryption Standard* (Berlin: Springer-Verlag, 2002). *https://doi.org/10.1007/978-3-662-60769-5*.

လျှို့ဝှက်ကုဒ်စနစ် (AES) စနစ်က သင့်ရဲ့ အချက်အလက် တွေကို blocks လို့ခေါ်တဲ့ အပိုင်းငယ်လေးတွေအဖြစ် ခွဲလိုက်ပြီးနောက် အဲဒီအပိုင်းငယ်တစ်ခုစီကို ရှုပ်ထွေးတဲ့ သင်္ချာနည်းစနစ်တွေနဲ့ လျှို့ဝှက်သော့ (secret key) ကို အသုံးပြုပြီး မွှေနှောက်လိုက်ခြင်းဖြင့် အလုပ်လုပ်ပါတယ်။ လျှို့ဝှက်သော့ (key) ကို ပို့ရှည်အောင် အသုံးပြုတာက စာဝှက်လျှို့ဝှက်ကုဒ်စနစ် (encryption) ကို ပိုကောင်းအောင် လုပ်တာမဟုတ်ပါဘူး။ ဒါပေမဲ့ စာဝှက်လျှို့ဝှက်ကုဒ်စနစ် (encryption) ကို ချိုးဖောက်ဖို့အတွက် လိုအပ်တဲ့ ခန့်မှန်း ရ မယ့် အရေအတွက်ကိုတော့ သိသိသာသာ အဆပေါင်းများစွာ တိုးလာစေပါတယ်။ အစွမ်းထက်တဲ့ ခေတ်မီကွန်ပျူတာ တွေနဲ့တောင် အချက်အလက်တွေကို လျှို့ဝှက်ကုဒ်အဖြစ်ပြောင်းလဲခြင်း စနစ် ကို အတင်းအဓမ္မဖောက်ဖျက်ဖို့အတွက် နှစ်သန်းပေါင်းများစွာ ကြာမြင့်နိုင်ပါတယ်။

လျှို့ဝှက်သော့တစ်မျိုးတည်းသုံးသောနည်း (Symmetric) နဲ့ မတူဘဲ လျှို့ဝှက်သော့ နှစ်မျိုးသုံးသော စာဝှက်လျှို့ဝှက်ကုဒ်စနစ် (asymmetric encryption) ကတော့ သော့တစ်ခု တည်းအစား သော့နှစ်ခုကို အသုံးပြုပါတယ်။ အဲဒီသော့နှစ်မျိုးမှာ အများသုံး (public) နဲ့ ကိုယ်ရေးကိုယ်တာသုံး (private) ဆိုတဲ့ အစိတ်အပိုင်းနှစ်ခုဖြစ်ပါတယ်။ အများသုံးသော့(public key) ကို လူတိုင်းက ပွင့်ပွင့်လင်းလင်း မျှဝေအသုံးပြုနိုင်ပြီး သတင်းအချက်အလက် စာသားတစ်ခုကို ကုဒ်ဝှက်ဖို့ အတွက်လည်း အသုံးပြုနိုင်ပါတယ်။ ဒါပေမဲ့ အဲဒီသတင်းအချက်အလက်စာသားကို ဖွင့်ဖို့ ဒါမှမဟုတ် ကုဒ်ပြန်ဖြေဖို့အတွက်တော့ တွဲဖက်ထားတဲ့ "private key" (လျှို့ဝှက်သော့) တစ်ခု တည်းကသာ လုပ်နိုင် ပါတယ်။ လျှို့ဝှက်သော့ နှစ်မျိုးသုံးသော စာဝှက်လျှို့ဝှက်ကုဒ်စနစ် (Asymmetric encryption) ဟာ ကုဒ်ဝှက်ထားတဲ့ သတင်းအချက် အလက်စာသားမပို့မီ သော့တစ်ခုတည်းကို လက်ခံသူမယ် သူနဲ့ မျှဝေရမယ့် ပြဿနာကို ဖြေရှင်းပေးပါတယ်[16] ။ တစ်နည်းအားဖြင့် ဒီနည်းဟာ မည်သူမဆို စာ ထည့်နိုင်တဲ့ စာတိုက်ပုံးတစ်ခုလိုမျိုး လုပ်ဆောင်ပါတယ်။ ဒါပေမဲ့ မှန်ကန်တဲ့ လျှို့ဝှက်သော့ (private key) ရှိတဲ့သူကသာ ပို့လိုက်တဲ့စာကို ဖတ်နိုင်ပါတယ်။ လျှို့ဝှက်သော့ (private keys) တွေကို ဘယ်တော့မှ ဖလှယ်တာ မရှိပါဘူး။ လျှို့ဝှက်သော့ နှစ်မျိုးသုံးသော စာဝှက်လျှို့ဝှက်ကုဒ်စနစ် (Asymmetric encryption) ရဲ့ အသုံးများတဲ့ ဥပမာတစ်ခုကတော့ လုံခြုံတဲ့ အချက်အလက် ပို့လွှတ်မှုတွေအတွက် အဓိကအသုံးပြုတဲ့ Rivest-Shamir-Adleman (RSA) [17] ပဲ ဖြစ်ပါတယ်။ ဘဲဥပုံမျဉ်းကွေးသုံး စာဝှက်စနစ် (Elliptic Curve Cryptography (ECC)) ဟာလည်း လျှို့ဝှက်သော့ နှစ်မျိုးသုံးသော စာဝှက်လျှို့ဝှက်ကုဒ်စနစ် (asymmetric encryption) ဥပမာတစ်ခု ဖြစ်ပါတယ်[18]။ ဒီစနစ်က RSA လိုပဲ လုံခြုံရေးအဆင့်အတန်းတူညီစွာ ပေးစွမ်းနိုင်ပေမဲ့ သော့အရွယ်အစား သေးငယ်တာကြောင့် ဆက်သွယ်ဆောင်ရွက်နိုင် စွမ်းအား နဲ့ အင်တာနက်အမြန်နှုန်း (bandwidth) အရ ပိုပြီး ထိရောက်မှု ရှိပါတယ်။

---

16 Annie Badman and Matthew Kosinski, “What is asymmetric encryption?,” *IBM*, August 8, 2024, https://www.ibm.com/think/topics/asymmetric-encryption.

17 Hemant Bhatt, “What is RSA? How does an RSA work?,” *Encryption Consulting*, March 4, 2024, https://www.encryptionconsulting.com/education-center/what-is-rsa/.

18 Rahul Awati and Andrew Froehlich, “What is elliptical curve cryptography (ECC)?,” *TechTarget*, Marc 17, 2025, https://www.techtarget.com/searchsecurity/definition/elliptical-curve-cryptography.

ဒီပေါ်မှာ ဆက်လက်ပြီးပြောရရင် OpenPGP ဟာ အီးမေးလ်ဝန်ဆောင်မှုတွေမှာ အသုံးအများဆုံး စာဝှက်လျှို့ဝှက် ကုဒ်စနစ် (encryption) စံနှုန်းတစ်ခု ဖြစ်ပါတယ်[19]။ OpenPGP ဟာ မူပိုင်ခွင့်ရှိတဲ့ PGP (Pretty Good Privacy) ကို အခြေခံထားတာဖြစ်ပြီး OpenPGP ကတော့ PGP protocol ရဲ့ မူပိုင်ခွင့်မရှိတဲ့ မူကွဲတစ်ခု ဖြစ်ပါတယ်[20]။ ဒါကြောင့် မူရင်း မူပိုင်ခွင့်ရှိတဲ့ PGP software အတွက် အခကြေးငွေပေးစရာမလိုဘဲ ဒီနည်းလမ်းကို ဘယ်သူမဆို အသုံးပြုနိုင်ပါတယ်။ Proton Mail နဲ့ Mailbox.org လိုမျိုး OpenPGP စံနှုန်းတွေကို ထောက်ပံ့ပေးတဲ့ အီးမေးလ်ဝန်ဆောင်မှုပေးသူတွေ အများအပြားရှိပါတယ်။ ဒါပေမဲ့ OpenPGP ဟာ အီးမေးလ်ရဲ့ ခေါင်းစဉ် (subject lines)၊ ပေးပို့သူ (sender) နဲ့ လက်ခံသူ (recipient) တို့ကိုတော့ မူရင်းအတိုင်း ကုဒ်ဝှက်ပေးထားခြင်း မရှိပါဘူး။

Public Key Infrastructure (PKI)

ကျွန်တော်တို့ဟာ တခြားနိုင်ငံကို လေယာဉ်နဲ့ မထွက်ခွာခင်မှာ ကိုယ် ဘယ်သူဘယ်ဝါဖြစ်တယ်ဆိုတဲ့ သက်သေအထောက်အထားကို တင်ပြဖို့ လိုအပ်ပါတယ်။ ယုံကြည်စိတ်ချရမှုရရှိဖို့အတွက် နိုင်ငံကူးလက်မှတ်၊ ဗီဇာနဲ့ တခြား တရားဝင်စာရွက်စာတမ်းတွေကို တင်ပြတာမျိုး လုပ်ရပါတယ်။ ဒီလိုယုံကြည်စိတ်ချရမှုမျိ အင်တာနက်ကွန်ရက် အသုံးပြုနေစဉ်မှာလည်း လိုအပ်ပါတယ်။ အင်တာနက်စာမျက်နှာတစ်ခုကို သင်ဝင်ရောက်တဲ့အခါ သင်ဟာ မှန်ကန်တဲ့ အဖွဲ့အစည်းနဲ့ ဆက်သွယ်နေတာ ဟုတ် မဟုတ်၊ သင့်ရဲ့ ဆက်သွယ်မှုတွေ လုံခြုံမှုရှိရဲ့လားဆိုတာကို သိရှိဖို့ လိုပါတယ်။ ဒီနေရာမှာ Public Key Infrastructure (PKI) စနစ်က အရေးပါလာပါတယ်။ PKI စနစ်က ဟာ အခြေခံအားဖြင့် ကျွန်တော်တို့ရဲ့ အွန်လိုင်းဆက်သွယ်မှုတွေကို လုံခြုံစေဖို့ အတွက် ထိန်းကြောင်းအုပ်ချုပ် ပေးတဲ့ မူဘောင်တစ်ခု ဖြစ်ပါတယ်။ ဒါဟာ လုံခြုံတဲ့ဆက်သွယ်မှုတွေ လုပ်နိုင်ဖို့အတွက် သုံးစွဲသူတွေရဲ့ ကိုယ်ပိုင်အချက်အလက်တွေကို သတ်မှတ်ခွဲဝေ၊ ရွေးထုတ်ခွဲခြား နဲ့ အတည်ပြုပေးတဲ့ နည်းပညာပိုင်း ဆိုင်ရာ လုပ်ငန်းစဉ်တစ်ခုဖြစ်သလို၊ မူဝါဒအစုအဝေးတစ်ခုလည်း ဖြစ်ပါတယ် [21]။

ဒီအမည်ကို သင်ရင်းနှီးမှုမရှိပေမဲ့ လက်တွေ့မှာတော့ PKI စနစ်နဲ့ လက်တွေ့ကြုံဖူးပြီး အသုံးပြုဖူးဖို့ အလွန်များပါတယ်။ သင် https:// အင်တာနက်စာမျက်နှာတစ်ခုကို ဝင်ရောက်တဲ့အခါ သင့်ရဲ့ ဘရောက်ဆာ (Browser) က အဲဒီအင်တာနက်စာမျက်နှာ ဟာ မည်သူမည်ဝါဖြစ်ကြောင်း ဆုံးဖြတ်ပေးတဲ့ အချက်အလက်တွေကို စစ်ဆေးအတည်ပြုဖို့ PKI စနစ်ကို အားထားရပါတယ်။ ဥပမာအားဖြင့် wikipedia.org ကို သင်ဝင်ရောက်တယ်ဆိုပါစို့။ သင့်ဘရောက်ဆာ (Browser) စာမျက်နှာ မှာ သော့ခလောက်ပုံစံ အိုင်ကွန်တစ်ခုကို တွေ့ရပါလိမ့်မယ်။ အဲဒီ ကို သော့ခလောက်ပုံစံ နှိပ်လိုက်ရင် သင့်ဘရောက်ဆာ (Brower) က Wikipedia ရဲ့ ဒစ်ဂျစ်တယ်လက်မှတ်အကြောင်း အသေးစိတ်ဖော်ပြထားတဲ့ စာသားဖော်ပြချက် လေးထောင့်တုံးလေးတစ်ခု ပွင့်လာပါလိမ့်မယ်။

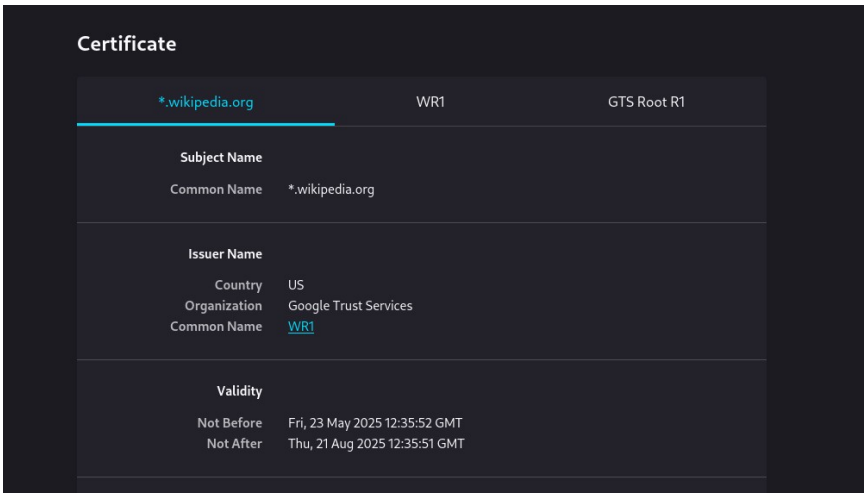
---

19 "About," OpenPGP, last modified September 29, 2024, https://www.openpgp.org/about/.

20 Michael Buckbee, "What is PGP encryption and how does it work?," *Varonis*, June 2, 2023, https://www.varonis.com/blog/pgp-encryption.

21 Josh Schneider and Ian Smalley, "What is public key infrastructure?," *IBM*, August 12, 2024, https://www.ibm.com/think/topics/public-key-infrastructure

အောက်ပါ နမူနာရိုက်ကူးထားတဲ့ပုံမှာပြထားတဲ့အတိုင်း Google Trust Services က ထုတ်ပေးထားတဲ့ ဒီလက်မှတ်မှာ သတ်မှတ်ထားတဲ့ အချိန်ကာလတစ်ခုအတွင်းပဲ အတည်ပြုနိုင်ပြီးတော့၊ wikipedia.org ဒိုမိန်းနဲ့ ကိုက်ညီတာတွေကို ကွန်တော်တို့ တွေ့မြင်နိုင်ပါတယ်။



ဓာတ်ပုံရှင်းလင်းချက်- Google Trust Services (WR1) မှ *.wikipedia.org အတွက် ထုတ်ပေးထားသော ဒစ်ဂျစ်တယ်လက်မှတ် မျက်နှာပြင်ပုံ ဖြစ်ပါသည်။ ၎င်းသည် ၂၀၂၅ ခုနှစ်၊ မေလ ၂၃ ရက်မှ ဩဂုတ်လ ၂၁ ရက်အထိ အကျုံးဝင်ပါသည်။

ဒီအသေးစိတ်အချက်အလက်တွေဟာ PKI စနစ် အဓိကဗဟိုမှာရှိတဲ့ လက်မှတ်ထုတ်ပေး ရေးအဖွဲ့ (Certificate Authority - CA) ကနေ ထုတ်ပေးထားတဲ့ လက်မှတ်ကနေ ရတာဖြစ်ပါတယ်။ လက်မှတ်ထုတ်ပေး ရေးအဖွဲ့ (CA) တွေဟာ ယုံကြည်စိတ်ချရတဲ့ တတိယအဖွဲ့အစည်း (trusted third party) အဖြစ် ဆောင်ရွက်ပြီး သတ်မှတ်ထားတဲ့ အများသုံးသော့ (public key) တစ်ခုဟာ အတည်ပြုပြီးသား အဖွဲ့အစည်းတစ်ခုရဲ့ ပိုင်ဆိုင်မှုဖြစ်ကြောင်း သက်သေခံတဲ့ ဒစ်ဂျစ်တယ်လက်မှတ်တွေကို ထုတ်ပေးပါတယ်[22]။ ဒီလုပ်ငန်းစဉ်က တစ်စုံတစ်ယောက်က လုံခြုံတဲ့ အင်တာနက်စာမျက်နှာတစ်ခုကို ဝင်ရောက်တဲ့အခါ ဒါမှမဟုတ် ဒစ်ဂျစ်တယ်လက်မှတ်နဲ့ ပို့ထားတဲ့ စာကို လက်ခံရရှိတဲ့အခါ အဲဒီအချက်အလက်တွေဟာ ကိုယ်မျှော်လင့်ထားတဲ့ အရင်း အမြစ်ကနေ လာတာဖြစ်ကြောင်း ယုံကြည်စိတ်ချနိုင်စေပါတယ်။ PKI စနစ်က သင့်ရဲ့အချက်အလက်တွေကို အယောင် ဆောင်ထားတဲ့ သို့မဟုတ် အန္တရာယ်ရှိတဲ့ အင်တာနက်စာမျက်နှာတစ်ခုဆီကို မသိဘဲ ပို့မိတာမျိုး မဖြစ်အောင်လည်း သေချာအောင် လုပ်ဆောင် ပေးပါတယ်။

[22] SSL Support Team, “What is Certificate Authority (CA)?,” SSL.com, January 5, 2024, https://www.ssl.com/article/what-is-a-certificate-authority-ca/

ခြိမ်းခြောက်မှုပုံစံကို ပုံဖော်လေ့လာခြင်း အခြေခံ ၁၀၁

ကိုယ်ရေးကိုယ်တာလုံခြုံမှု (privacy) ပိုမိုရရှိစေဖို့အတွက် အကြံဉာဏ်တွေ ရှာဖို့ သီးသန့် တည်ရှိနေတဲ့ ဖိုရမ်တွေထဲ ဝင်ကြည့်တဲ့အခါ သင်ဟာ ရှုပ်ထွေးနက်နဲတဲ့ အကြောင်းအရာတွေထဲ ကြားမှာ လမ်းပျောက်သွားနိုင်ပါတယ်။ ရုတ်တရက် ဆိုသလို သင်ဟာ အရာအားလုံးကို လျှို့ဝှက်ကုဒ်အဖြစ်ပြောင်းလဲဖို့ ၊ အမည်မဖော်လိုတဲ့ ကိရိယာ ၁၀ ခုလောက် အသုံးပြုဖို့၊ အင်တာနက်လူမှုကွန်ရက်တွေအားလုံးကို ရှောင်ကြဉ်ဖို့နဲ့ ဒီကွန်ရက်ပြင်ပမှာပဲ အသက်ရှင်နေထိုင်ဖို့ လိုအပ် နေတယ်လို့ ခံစားလာရနိုင်ပါတယ်။ ဒီလိုခံစားရတာက မှန်ကန်ပါတယ်။ အထူးသဖြင့် သင်ဟာ ထိရှလွယ်တဲ့ ကိစ္စရပ်တွေကို လုပ်ဆောင်နေတာ ဒါမှမဟုတ် လူ့အဖွဲ့အစည်းထဲက အင်အားကြီးမားတဲ့ အဖွဲ့အစည်းတွေကို စိန်ခေါ် တွန်းလှန်နေတဲ့အခါမျိုးမှာဆို ပိုပြီး မှန်ကန်ပါတယ်။ ဒါဟာ လှုပ်ရှားတက်ကြွသူတွေအတွက် နေ့စဉ်ဘဝလိုမျိုး ဖြစ်နေ ပါတယ်။

ဒါကြောင့် ခြိမ်းခြောက်မှု ပုံစံနမူနာ (Threat Modelling) ရဲ့ သဘောတရားကို အပြည့်အဝနားလည်ထားဖို့ အရေးကြီးပါတယ်။ ဒစ်ဂျစ်တယ်လုံခြုံရေးဆိုတာ လုံးဝဥဿုံ ပြီးပြည့်စုံနေဖို့ မဟုတ်ပါဘူး။ အဓိက ရည်ရွယ်ချက်က သင်ဘာကို ကာကွယ်ချင်တယ်ဆိုတာရယ်၊ ဘယ်သူဆီကနေ ကာကွယ်ချင်တယ် ဆိုတာရယ်၊ ကာကွယ်ဖို့အတွက် ဘယ်လောက်အထိ အားထုတ်မှု ဒါမှမဟုတ် အရင်းအမြစ်တွေကို ရင်းနှီးမြှုပ်နှံဖို့ ဆန္ဒရှိလဲ သို့မဟုတ် တတ်နိုင်လဲဆို တာကို နားလည်ဖို့ပဲ ဖြစ်ပါတယ်[23]။ အစကတည်းက တန်းပြီးလုပ်ဆောင်မယ်ဆိုရင် သင့်ရဲ့ အမှန်တကယ်အန္တရာယ်နဲ့ မကိုက်ညီတဲ့ ကာကွယ်လုပ် ဆောင်မှုတွေမှာ အချိန်ဖြုန်းတာမျိုး ဒါမှမဟုတ် ပိုဆိုးတာက တကယ်အရေးကြီးတဲ့ အရာတွေကို လစ်လျူရှုမိ တာမျိုးတွေ ဖြစ်နိုင်ပါတယ်။ အောက်မှာဖော်ပြထားတာတွေကတော့ Tashea ကြိုးစားပြုစု ထားတဲ့အရာတွေကို ကိုးကားပြီး သင့်ရဲ့ ဒစ်ဂျစ်တယ်လုံခြုံရေး ခရီးစဉ်မှာ အထောက်အကူဖြစ်စေဖို့အတွက် သင့်ကိုယ်သင် မေးနိုင်တဲ့ မေးခွန်းတွေပဲ ဖြစ်ပါတယ်[24]။

ဇယားနံပါတ် (၁)- ခြိမ်းခြောက်မှု ပုံစံနမူနာ အတွက်မေးခွန်းများ

မေးခွန်း	**နောက်ဆက်တွဲ မေးခွန်းများ**
ကျွန်တော် ဘာကို ကာကွယ်ဖို့ ကြိုးစားနေတာလဲ။	ပိုင်ဆိုင်မှုတွေလား။ ကိုယ်ရေးကိုယ်တာ အချက်အလက် တွေလား။ စသဖြင့်ပေါ့။
ကျွန်တော် ဘယ်သူ့ဆီကနေ ကာကွယ်ဖို့ ကြိုးစားနေ တာလဲ။	အစိုးရလား။ မာ့ခ်ဇူကာဘတ ် (Mark Zuckerberg) လား။ အကြမ်းဖက်တတ်တ ဲ့ လက်တွဲဖော်လား။ စပ်စုတတ်တဲ့ အိမ်နီးချင်းလား။
အချက်အလက်ပေါက်ကြားမှု ဖြစ်ပေါ်လာပါက နောက်ဆက်တွဲ	လူတွေကို အန္တရာယ်ဖြစ်စေမှာလား။ ဂုဏ်သိက္ခာကို ထိခိုက်စေမှာ

[23] Electronic Frontiers Foundation, “Threat Model,” Surveillance Self-Defense, accessed June 13, 2025, https://ssd.eff.org/glossary/threat-model

[24] Jason Tashea, “Stay safe out there: Threat modeling for campaigners”, *Mobilisation Lab*, August 12, 2015, https://mobilisationlab.org/stories/threat-modeling-for-campaigners-and-activists/; Electronic Frontiers Foundation, “Your Security Plan,” Surveillance Self-Defense, p*ublished October 27, 2023*, https://ssd.eff.org/module/your-security-plan.

ပြဿနာများက ဘာတွေလဲ။	လား။ ကျွန်တော် ကိုယ့်ကိုယ်ကို သို့မဟုတ် တခြားသူတွေရဲ့ ကိုယ်ရေးကိုယ်တာအချက်အလက် တွေ အင်တာနက်ကွန်ရက်ပေါ်မှာ ဖွင့်ချသလို ဖြစ်စေမှာလား။
အန္တရာယ်ခြိမ်းခြောက်မှုက တကယ်တမ်း ဖြစ်လာနိုင်ခြေ ဘယ်လောက်ရှိပါသလဲ။	ကျွန်တော့်အတွက် ခြိမ်းခြောက်မှုတွေက လက်တွေ့ကျ ပြီး ခိုင်မာတဲ့ သက်သေအထောက်အထား တွေအပေါ် အခြေခံထားတဲ့ အန္တရာယ်တွေ ဟုတ်ပါသလား။
ကျွန်တော် ဘယ်လောက်အထိ အားထုတ်ဖို့ ဒါမှမဟုတ် ဘယ်လောက်သုံးပြီး ရင်းနှီးမြှုပ်နှံဖို့ ဆန္ဒရှိလဲ သို့မဟုတ် တတ်နိုင်လဲ။	ကျွန်တော်မှာ လိုအပ်တဲ့ လုံခြုံရေးအစီအမံတွေကို အကောင်အထည်ဖော်ပြီး ထိန်းသိမ်းဖို့အတွက် အချိန်၊ ကျွမ်းကျင်မှု၊ ငွေကြေး ဒါမှမဟုတ် အကူအညီပေးနိုင် မယ့် ကွန်ရက် ရှိပါသလား။

ပထမဆုံးမေးခွန်းကတော့ "ကျွန်တော် ဘာကို ကာကွယ်ဖို့ ကြိုးစားနေတာလဲ" ဆိုတာ ဖြစ်ပြီး ဒီမေးခွန်းဟာ သင့်ရဲ့ လုံခြုံရေးဗျူဟာတစ်ခုလုံးရဲ့ အခြေခံအုတ်မြစ် ဖြစ်ပါတယ်။ ဒုတိယအကွက် မှာတော့ ဒီအကြောင်းအရာနဲ့ ပတ်သက်ပြီး ဆက်လက်ဆွေးနွေးမှုစတင်နိုင်ဖို့ ကူညီပေးနိုင်တဲ့ နောက်ဆက်တွဲမေးခွန်းတွေကို ကျွန်တော်တို့ ထည့်သွင်း ပေးထား ပါတယ်။ သင့်ရဲ့ ရုပ်ပိုင်းဆိုင်ရာ လုံခြုံမှုကို ကာကွယ်နေတာလား။ ဒါမှမဟုတ် အကျင့်ပျက်ခြစားမှုနဲ့ ပတ်သက်တဲ့ အရာရှိတွေ အပေါ် တရားစွဲဆိုဖို့အတွက် နောင်တစ်ချိန်မှာအသုံးပြုဖို့ စီစဉ်ထားတဲ့ အရေးကြီးစာရွက် စာတမ်းတစ်ခုလား။ ဒါမှမဟုတ် သင့်ရဲ့ အဓိကအာရုံက သက်သေခံ အချက်အလက်ဖော်ထုတ်တိုင်ကြားလိုသူတွေ ကို ဘယ်သူဘယ်ဝါဖြစ်ကြောင်း ဆုံးဖြတ်ပေးနိုင်တဲ့ သူတို့ရဲ့ ကိုယ်ရေးကိုယ်တာ အချက်အလက်တွေနဲ့ ဆက်သွယ်မှုတွေကို မလိုလားအပ်တဲ့ ပေါက်ကြား မှုတွေကနေ ကာကွယ်ဖို့ လား။ ဒီမေးခွန်းကို ရှင်းရှင်းလင်းလင်း ဖြေဖို့ဆိုရင် သုံးသပ်တွေးခေါ်မှု လိုအပ်ပါတယ်။ ဘာလို့လဲဆိုတော့ အပေါ်ယံကြည့်ရုံနဲ့ မသိနိုင်တဲ့ ဒုတိယအဆင့် ပိုင်ဆိုင်မှုတွေ ရှိနေနိုင်လို့ပါပဲ။ ဥပမာအနေနဲ့ ရဲတွေရဲ့ ရက်စက်ကြမ်းကြုတ်မှုကို မှတ်တမ်းတင်ထားတဲ့ ဗီဒီယိုဖိုင်တစ်ခုကို သင်ပိုင်ဆိုင်ထားတယ်ဆိုပါစို့။ ထင်ထင်ရှားရှားပဲ၊ ဒီဗီဒီယိုထဲမှာ လိုအပ်တဲ့ သက်သေအထောက်အထားတွေ ပါဝင်နေတာကြောင့် သင်ဟာ ဗီဒီယိုကိုယ်တိုင်ကို ကာကွယ်ချင်ပါလိမ့်မယ်။ ဒါပေမဲ့ တကယ်တမ်းမှာတော့ ဗီဒီယိုကိုယ်တိုင်ကို ကာကွယ်ခြင်းအားဖြင့် ဗီဒီယိုထဲက လူတွေကို၊ အဲဒါကို ရိုက်ကူးခဲ့တဲ့ အချိန်နဲ့နေရာကို ကာကွယ်ထားသလိုဖြစ်နေပြီး ၊ ဒီဗီဒီယို သိမ်းဆည်းထားတဲ့ စက်ပစ္စည်း နဲ့ သတင်းထောက်တစ်ယောက် ဆီကို ပို့နိုင်မယ့် လမ်းကြောင်းကိုပါ ကာကွယ်နေတာ ဖြစ်ပါတယ်။ ဖိုင်တစ်ခုဆိုတာ ပိုင်ဆိုင်မှုပစ္စည်းတစ်ခုတည်းသက်သက် မဟုတ်ပါဘူး။ အဲဒီထဲမှာ တူညီတဲ့ဂရုစိုက်မှုနဲ့ ကြိုတင် ကာကွယ်မှုတွေ လိုအပ်တဲ့ ထိလွယ်ရှလွယ် အစိတ်အပိုင်းပေါင်းစုံ ပါဝင်ပါတယ်။ ပိုင်ဆိုင်မှုပစ္စည်းတိုင်းဟာ တခြားသော ပိုင်ဆိုင်မှုပစ္စည်းတွေရဲ့ အလွှာများစွာနဲ့ ဆက်စပ်ဖွဲ့စည်းထား တယ်ဆိုတာကို နားလည်ထားခြင်းအားဖြင့် သင်ကို အမြင်ကျဉ်း မြောင်းမှု/ဘက်တစ်ဘက်ကို မြင်နိုင်မှု ကာကွယ်ပေး ပါလိမ့်မယ်။

ဒီတစ်ခါမှာတော့ သင်ကာကွယ်ဖို့ ကြိုးစားနေတဲ့ အရာကို ပိုပြီးနားလည်နိုင်ဖို့ ဒုတိယမေးခွန်းနဲ့ ပိုနက်နက်ရှိုင်းရှိုင်း ဆွေးနွေးကြည့်ရအောင်။ သင့်သင်ကာကွယ်ဖို့ ကြိုးစားနေတဲ့ အရာက ရုပ်ပိုင်းဆိုင်ရာနဲ့ပတ်သတ်တဲ့ လုံခြုံရေးဆိုရင် အဲဒီ အန္တရာယ်ခြိမ်းခြောက်မှုက အဆင့်မြင့်တဲ့ စောင့်ကြည့်ရေးကိရိယာတွေရှိတဲ့ နိုင်ငံတော်

အာဏာပိုင်တွေဆီက လာတာလား၊ ဒါမှမဟုတ် အကြမ်းဖက်တတ်တဲ့ လက်တွဲဖော်လိုမျိုး ပိုပြီးနီးစပ်တဲ့ ပုဂ္ဂိုလ်တစ်ဦးဆီကလာတာလား ဆိုတာကို စဉ်းစားဖို့ လိုအပ်ပါတယ်။ အန္တရာယ်ခြိမ်းခြောက်မှုရဲ့အရင်းခံက မည်သူမည်ဝါဖြစ်ကြောင်း တိတိကျကျ သိရှိခြင်းက သင့်ရဲ့ကာကွယ်ရေး နည်းဗျူဟာတွေကို ခြိမ်းခြောက်မှုတွေနဲ့ကိုက်ညီအောင် လုပ်ဆောင်နိုင်ပါလိမ့်မယ်။ သင့်ရဲ့ တန်ပြန်ကာကွယ် တုံ့ပြန်မှုတွေဟာ ခြိမ်းခြောက်သူရဲ့စွမ်းဆောင်ရည်နဲ့ နီးစပ်မှုအတိုင်းအတာအလိုက် တန်းတူ ရှိသင့်/ရသင့်ပါတယ်။ သင့်ကို ခြိမ်းခြောက်သူက အစိုးရဖြစ်နေမယ်ဆိုရင် သင်ဟာ ဖုန်းပြောတာတွေကို ခိုးနားထောင်တာ၊ စောင့်ကြည့်ရေး ဒရုန်းတွေ ဒါမှမဟုတ် လျှို့ဝှက်ခြေရာခံဆော့ဖ်ဝဲ (Pegasus spyware) တွေနဲ့ ရင်ဆိုင်ရနိုင်ပါတယ်။ ဒါပေမဲ့ ခြိမ်းခြောက်သူက အကြမ်းဖက်တတ်တဲ့ လက်တွဲဖော်ဖြစ်နေမယ်ဆိုရင်တော့ အန္တရာယ်က ပိုပြီးပုဂ္ဂိုလ်ရေးဆန်ကာ ချက်ချင်းလက်ငင်း၊ ကိုယ့်အနီးအနားကနေပဲ ဖြစ်နိုင်ခြေပိုများပါတယ်။ ဒီအန္တရာယ်ဟာ သင့်ရဲ့ပစ္စည်းကိရိယာတွေကို ကိုယ်တိုင်ယူပြီး စောင့်ကြည့်တာမျိုးနဲ့ အင်တာနက်လူမှုကွန်ရက်တွေက လှုပ်ရှားမှုတွေကို စောင့်ကြည့်တာမျိုး ဖြစ်လာနိုင်ပါတယ်။

တတိယမေးခွန်းကတော့ အဖြေပေးဖို့ အခက်ခဲဆုံးဖြစ်နိုင်ပါတယ်။ ဘာလို့လဲဆိုတော့ အဲဒီမေးခွန်းက ကြောက်ရွံ့တာတို့ ၊ နောင်တရနေတာတို့ မဖြစ်ဘဲနဲ့ အနာဂတ်ကို ကြိုပြီး မျှော်တွေးနိုင်တဲ့ ကျွမ်းကျင်မှုမျိုး အသုံးပြုဖို့ လိုအပ်လို့ပဲ ဖြစ်ပါတယ်။ ဒါဟာ အချက်အလက်ပေါက်ကြားမှုအတွက်ကြောင့် ရှေ့ဖြစ်လာမှာတွေအတွက် ကြိုတင်ပြီး ကိုယ့်ကိုယ်ကိုယ် အပြစ်တင်နေရမယ့်အချိန် မဟုတ်ပါဘူး။ ဒီအချိန် ဟာ သင့်ကိုယ်သင် ရိုးသားဖို့နဲ့ ပျက်စီးဆုံးရှုံးမှု တစ်စုံတစ်ရာမဖြစ်ခင်မှာ တာဝန်ယူမှု ၊ တာဝန်ခံမှု ယူရမယ့် အတွက် အချိန်ဖြစ်ပါတယ်။ ဒီမေးခွန်းမှာ အရင်နှစ်ခုလို "I" (ငါ) ဆိုတဲ့စကားလုံး မပါရတဲ့အကြောင်းရင်းရှိပါတယ်။ ဒါက တာဝန်ယူမှုနဲ့ တာဝန်ခံမှုကို ကျွန်တော်တို့ မယုံကြည်လို့ မဟုတ်ပါဘူး။ စနစ်အလိုက်ဖြစ်တဲ့ ချို့ယွင်းချက်တွေဟာ တစ်ဦးချင်းရဲ့အမှားတွေ သက်သက်ထက် လုံခြုံရေးပြိုကွဲမှုတွေရဲ့ အဓိကအကြောင်းအရင်းဖြစ်တယ်လို့ ကျွန်တော်တို့ ယုံကြည်လို့ပဲဖြစ်ပါတယ်။ တတိယမေးခွန်းက ရှင်းရှင်းလင်းလင်း၊ ရည်ရွယ်ချက်ရှိရှိနဲ့ ရှေ့ကိုကြိုပြင်ဆင်နိုင်ဖို့ အတွက် သင့်ကိုတွန်းအား ပေးစေနိုင်ပါတယ်။ ဒီမေးခွန်းက တစ်ခုခုမဖြစ်ခင်မှာ ဘာတွေဖြစ်လာနိုင်လဲဆိုတာကို နားလည်စေဖို့ ကူညီပေးပါတယ်။ ဒီလိုရေးဆွဲချမှတ်ခြင်းအားဖြင့် သင်ဟာ အမြော်အမြင်ရှိရှိနဲ့ တာဝန်ယူမှုရှိရှိ လုပ်ဆောင်နိုင်ဖို့ ကိုယ့်ကိုယ်ကိုယ် နေရာချ ပြင်ဆင်ထားခြင်းဖြစ်ပါတယ်။ ဒါဟာ လက်တွေ့ကျတဲ့ ဦးဆောင်မှုပါပဲ။

နောက်ဆုံးမေးခွန်းနှစ်ခုက မကြာခဏဆိုသလို တွဲလျက်လာတတ်ပါတယ်။ ဘာကြောင့်လဲဆိုတော့ ခြိမ်းခြောက်မှု ဖြစ်လာနိုင်ခြေက သင့်လုံခြုံရေးအတွက် သင် အချိန်ဘယ်လောက်နဲ့ ကြိုးစားအားထုတ်မှုဘယ်လောက် စိုက်ထုတ်ချင်လဲ ၊လိုအပ်တယ်ဆိုတာ အသိပေးလို့နိုင်ပဲဖြစ်ပါတယ်။ ဒါတွေဟာ ကျွန်တော်တို့ အမြဲတစေ ပြန်လည်သုံးသပ်နေရတဲ့ မေးခွန်းတွေပါ။ သတိတရား နဲ့ စွမ်းဆောင်ရည်ကြားက မှန်ကန်မျှတတဲ့ အခြေအနေတစ်ခုကို ရရှိနိုင်ဖို့ ကြိုးစားရင်း ဒီမေးခွန်းတွေကို ကျွန်တော်တို့ ခေါင်းထဲမှာ အကြိမ်ကြိမ်အခါခါ တွေးနေရတတ်ပါတယ်။ ဒါပေမဲ့ ဖြစ်နိုင်ခြေရှိတယ်လို့ သင်ယူဆတာဟာ သင့်ရဲ့စိုးရိမ်ပူပန်မှုတစ်ခုတည်းအပေါ်မှာပဲ မမူတည်

သင့်ပါဘူး။ သို့ပေမယ့်လည်း စိုးရိမ်ပူပန်မှုဆိုတာ လူသားတို့ရဲ့ ဖြစ်လေ့ဖြစ်ထရှိတဲ့ ခံစားချက်တစ်ခုဖြစ်ကြောင်း ကျွန်တော်တို့ နားလည်ပါတယ်။ လတ်တလောရုပ်သံတွေမှာ မြင်နေရတဲ့အရာတွေအားလုံးကြောင့် ကမ္ဘာကြီးနဲ့ ပတ်သက်ပြီး စိုးရိမ်ပူပန်တာဟာ ပုံမှန်ပါပဲ။ အထူးသဖြင့် သင်ဟာ အန္တရာယ်များတဲ့ ပတ်ဝန်းကျင်တွေမှာ အလုပ်လုပ်နေရရင်ပေါ့။ ဒါပေမဲ့ စိုးရိမ်ပူပန်မှုဆိုတာ သက်သေအထောက် အထား နဲ့တော့ မတူပါဘူး။

စတုတ္ထမေးခွန်းကို ရှင်းရှင်းလင်းလင်းဖြေဆိုနိုင်ဖို့ သင်ဟာ အနည်းငယ်နောက်ဆုတ်ပြီး ခြိမ်းခြောက်မှုဖြစ်လာနိုင်ခြေကို အကဲဖြတ်ရပါမယ်။ သင့်ရဲ့ကွန်ရက် ဒါမှမဟုတ် လှုပ်ရှားမှုတွေမှာ အလားတူဖြစ်ရပ်တွေ ရှိခဲ့ဖူးပါသလား။ သင့်စီရောက်လာတဲ့ ခြိမ်းခြောက်မှုပုံစံဟာ လက်တွေ့ကျပြီး သေချာနေပြီလို့ ယူဆနိုင်တဲ့ ထပ်ခါထပ်ခါ လုပ်ဆောင်နေတဲ့ စောင့်ကြည့်မှု ဒါမှမဟုတ် ပစ်မှတ်ထားခံရမှုပုံစံတွေ ရှိခဲ့ဖူးပါသလား။ အရာရာတိုင်းအတွက် ပထမဆုံးအကြိမ်ဆိုတာ အမြဲရှိနေနိုင်ပြီး၊ ခြိမ်းခြောက်မှုတွေ အမှန်တကယ်အသက်မဝင်လာခင်အထိတော့ ကိုယ်ပစ်မှတ်ထားခံနေရတယ်ဆိုတာ မသိနိုင်တာလည်း မကြာခဏဖြစ်တတ်ပါတယ် ။ ခြိမ်းခြောက်မှုနဲ့ပတ်သတ်တဲ့ သက်သေအထောက်အထားမရှိခြင်းကို အန္တရာယ် မရှိဘူးလို့ ယူဆပြီး ပေါ့ပေါ့ဆဆ မနေသင့်ပါဘူး။ အဲ့ဒီအစား သင့်ရဲ့ကာကွယ်ရေးကို ဘယ်လိုဦးစားပေးပြီး လိုက်လျောညီထွေဖြစ်အောင် ဘယ်လိုနေရမလဲဆိုတာကို ပြောင်းလဲပေးသင့်ပါတယ်။ ဒီလိုအခြေအနေက ကျွန်တော် တို့ကို နောက်ဆုံးမေးခွန်းဆီသို့ ဦးတည်စေပါတယ်။ သင် ဘယ်လောက်အထိ အားထုတ်ဖို့ ဒါမှမဟုတ် ဘယ်လောက်သုံးပြီး ရင်းနှီးမြှုပ်နှံဖို့ ဆန္ဒရှိလဲ သို့မဟုတ် တတ်နိုင်လဲ။ အမှန်တကယ် သင်ဘယ်လောက်လုပ်ဆောင် နိုင်လဲ၊ လက်လှမ်းမီနိုင်တဲ့ ရှိပြီးသားကွန်ရက်တွေကို ဘယ်လောက်လက်လှမ်းမှီလဲ ၊ ငွေကြေး စိုက်ထုတ်နိုင်အား ဆိုတာ တွေက အရင်ကမေးခဲ့တဲ့ မေးခွန်းအားလုံးကို သင် ဖြေဆိုဖို့ အထောက်အကူဖြစ်ပါလိမ့်မယ်။ သင်လိုချင်တာဟာ ရေရှည် တည်တံပြီး ယုံကြည်စိတ်ချရတဲ့ နည်းဗျူဟာတစ်ခုဖြစ်ပါလိမ့်မယ်။

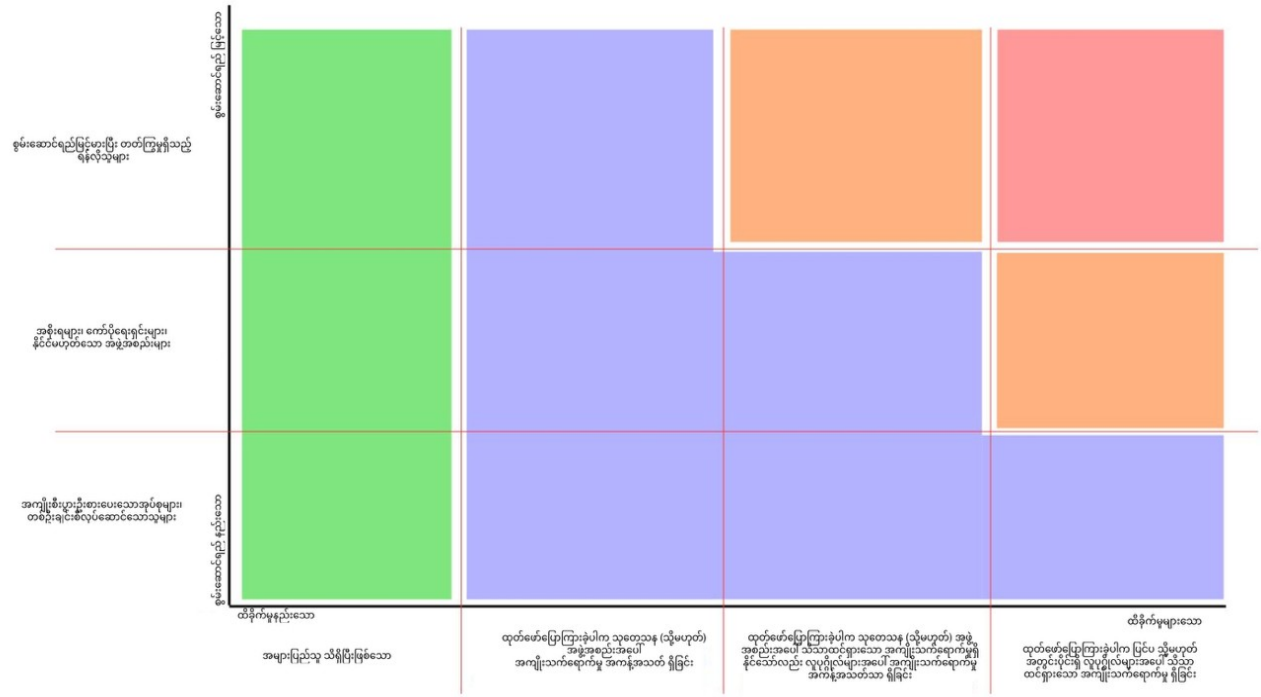
ဆမ်းမက် (Sammut) ရဲ့ လုံခြုံသောဆက်သွယ်ရေးမူဘောင် (Secure Communications Framework-SCF)

သင့်ရင်ဆိုင်နေရတဲ့ ခြိမ်းခြောက်မှုနဲ့ အန္တရာယ်အခြေအနေ ကို အကဲဖြတ်နိုင်ဖို့ ကူညီပေးမယ့် မူဘောင်တစ်ခုကတော့ Tim Sammut ရဲ့ လုံခြုံသောဆက်သွယ်ရေးမူဘောင် (Secure Communications Framework-SCF) ဖြစ်ပါတယ်[25]။ Sammut က ဒီမူဘောင်ကို လူ့အခွင့်အရေးတတ်ကြွလှုပ်ရှားသူတွေအနေနဲ့ သူတို့ရဲ့သတင်းအချက်အလက်တွေက ဘယ်လောက်အထိ ထိလွယ်ရှလွယ်နေသလဲ၊ သူတို့ ဘယ်လိုကာကွယ်မှုမျိုးတွေ လိုအပ်သလဲဆိုတာကို ဝေဖန်ပိုင်းခြား ပြီး ဆန်းစစ်နိုင်ဖို့ ရည်ရွယ်ဖန်တီးခဲ့တာ ဖြစ်ပါတယ်။ ဒီမူဘောင်က ခြိမ်းခြောက်မှုပုံစံကိုပုံဖော်လေ့လာခြင်းက (threat modelling) မေးခွန်းတွေနဲ့ ဆင်တူပေမဲ့ အန္တရာယ်ကို မြင်သာစေဖို့ အတွက် ဇယားကွက် ပုံစံနဲ့ ပြသထားပါတယ်။ ဇယားကွက်ရဲ့ ရေပြင်ညီမျဉ်း ဟာဆိုရင် အများသူငါ လက်လှမ်းမှီတဲ့ ထိလွယ်ရှလွယ် ခံနိုင် တဲ့ အချက်အလက်ကနေစပြီး ပိုမိုထိခိုက်လွယ်တဲ့၊ ပေါက်ကြားသွားပါက

[25] Tim Sammut, “Secure Communications Framework,” Teamsammut (blog), March 04, 2016, https://teamsammut.com/scf/.

တစ်ဦးတစ်ယောက်ချင်းအပေါ် ကြီးကြီးမားမား သက်ရောက်မှုရှိနိုင်တဲ့ အချက်အလက်တွေအထိ သင့်ရဲ့ သတင်းအချက်အလက်တွေရဲ့ ထိလွယ်ရှလွယ်အဆင့်သတ်မှတ်ချက်ကို ဖော်ပြပါတယ်။ ဆန့်ကျင်ဘက်အားဖြင့် ဇယားကွက်ရဲ့ ထောက်လိုက်မျဉ်း ကတော့ သင့်ရဲ့ အလားအလာရှိတဲ့ရန်သူတွေ ဘယ်လောက် အစွမ်းထက်ပြီး၊ စွမ်းဆောင်ရည်ဘယ်လောက်ရှိလဲဆိုတာကို ပြသပါတယ်။ ဒီတိုင်းတာနိုင်တဲ့ အရာနှစ်ခုဟာ ခြိမ်းခြောက်မှုပုံစံ မိတ်ဆက်ရဲ့ မေးခွန်း ၂ နဲ့ ၃ တို့နဲ့ တော်တော်လေးနီးနီးစပ်စပ်နဲ့ ကို ဆက်စပ်နေပါတယ်။

ဒီမူဘောင်ရဲ့ အထောက်အကူဖြစ်စေနိုင်တဲ့အချက်ကတော့ ပြီးပြည့်စုံတဲ့ဖြေရှင်းနည်း ဒါမှမဟုတ် အကြံဉာဏ်ပေးတာ မျိုး မဟုတ်ဘဲ ဖြစ်လာနိုင်တဲ့အန္တရာယ်နဲ့ပတ်သက်ပြီး ရှင်းရှင်းလင်းလင်းစဉ်းစားတွေးတောနိုင်အောင် ကူညီပေးတဲ့ အတွက် သင့်အချိန်နဲ့ ကြိုးစားအားထုတ်မှုတွေကို ပိုပြီးညဏ်ရှိရှိ အသုံးပြုနိုင်စေတာပဲ ဖြစ်ပါတယ်။ ဆမ်းမက် (Sammut) က လုံခြုံသောဆက်သွယ်ရေးမူဘောင် (SCF) ကို အခြေအနေအချို့မှာ 'ရှိရင်းစွဲအတိုင်း' အသုံးပြုလို့ မရနိုင်ဘူးဆိုတာ ကိုလည်း အသိအမှတ်ပြုထားပြီး လူတွေကို သူတို့ရဲ့လက်တွေ့အခြေအနေနဲ့ကိုက်ညီအောင် လုံခြုံသောဆက်သွယ်ရေး မူဘောင် (SCF) ကို ပြုပြင်ပြောင်းလဲသုံးစွဲဖို့ တိုက်တွန်းထားပါတယ်။.



ဓာတ်ပုံရှင်းလင်းချက်- Tim Sammut ၏ လုံခြုံသောဆက်သွယ်ရေးမူဘောင် Secure Communications Framework မှ အရောင်သုံးပြီး အန္တရာယ်အဆင့်သတ်မှတ်ထားသည့် ဇယားပုံဖြစ်သည်။ ဤဇယားသည် အချက်အလက်၏ အရေးကြီးမှု (နည်းရာမှ များရာသို့) အဆင့်နှင့် တိုက်ခိုက်သူ၏ စွမ်းဆောင်ရည် (နည်းရာမှ များရာသို့) အဆင့်ကို ပြသထားသည်။ အစိမ်းရောင်သည် အန္တရာယ်နည်းသော အဆင့်ကို ညွှန်ပြပြီး အပြာရောင်သည် အသင့်အတင့် ကြိုတင်ကာကွယ်ရန် လိုအပ်ကြောင်း၊ လိမ္မော်ရောင်သည် ပိုမိုခိုင်မာသော လုံခြုံရေးလိုအပ်ကြောင်းနှင့် အနီရောင်သည် ကျွမ်းကျင်သူ၏ အကူအညီလိုအပ်သော အန္တရာယ်ရှိ အဆင့်ကို

ဖြစ်စဉ်လေ့လာမှု - Arturo

ခြိမ်းခြောက်မှုပုံစံကို လက်တွေ့မှာ ဘယ်လိုပုံစံရှိမလဲဆိုတာ ပုံဖော်ပြီး လေ့လာဆန်းစစ်မှုဖို့အတွက် ဖြစ်စဉ် လေ့လာမှုတစ်ခုကို ကျွန်တော်တို့ ဖန်တီးထားပါတယ်။ ဒီနေရာမှာ ရှင်းလင်းသတိပေးလိုတာကတော့ အမည်နဲ့ ဇာတ်လမ်းကို ဒီဥပမာအတွက်ပဲ စိတ်ကူးနဲ့ ဖန်တီးထားတာဖြစ်ပါတယ်။ တကယ့်အပြင်မှာရှိလူပုဂ္ဂိုလ်တွေ (အသက်ရှင်နေဆဲဖြစ်စေ၊ သေပြီးဖြစ်စေ) ၊ အမှန်တကယ်ဖြစ်ရပ်တွေနဲ့ တိုက်ဆိုင်မှုရှိခဲ့ရင်တောင် ဒါဟာ လုံးဝကို တိုက်ဆိုင်မှု သာ ဖြစ်ပါတယ်။

လူအခွင့်အရေးလှုပ်ရှားသူတစ်ဦးဖြစ်တဲ့ အာတူရိုဟာ ဖိလစ်ပိုင်နိုင်ငံသားတစ်ဦးပါ။ ဖိလစ်ပိုင်မှာ 'Red-tagging' လို့ခေါ်တဲ့ တက်ကြွလှုပ်ရှားသူတွေနဲ့ အတိုက်အခံတွေကို အကြမ်းဖက်သမား၊ အဖျက်သမား၊ ကွန်မြူနစ် တံဆိပ်တပ်ခြင်းတွေ လုပ်လေ့ရှိပါတယ်။ 'Red-tagging' ဆိုတာကတော့ သက်သေအထောက်အထားမရှိဘဲ လူတွေကို လက်ဝဲစွန်း အကြမ်းဖက်သူတွေနဲ့ ဆက်စပ်မှုရှိတယ်လို့ စွပ်စွဲတာဖြစ်ပါတယ်။ အစိုးရအနေနဲ့ အတိုက်အခံဝေဖန်သူတွေကို နှုတ်ဆိတ်အသံတိတ်သွားအောင်လုပ်ဖို့နဲ့ ဒီပြဿနာဟာ နိုင်ငံတော်လုံခြုံရေး အတွက် ဖြစ်တယ်လို့ ပုံဖော်ကာ လူအများရဲ့သဘောတူညီချက်ရယူဖို့အတွက် ဒီ 'Red-tagging' နည်းလမ်းကို လက်နက် သဖွယ် အသုံးပြုခဲ့ကြပါတယ်။ ဒီလိုမျိုး တံဆိပ်ကပ်ခံရတဲ့အတွက် တက်ကြွလှုပ်ရှားသူတွေနဲ့ အတိုက်အခံတွေ ကိုတွေဟာ မကြာခဏဆိုသလို မတရား ဖမ်းဆီး ခံရတာ၊ ပျောက်ဆုံးသွားတာ (desaparacidos) ဒါမှမဟုတ် တရားလက်လွတ် သတ်ဖြတ်ခံရတာတွေနဲ့ ရင်ဆိုင် ရလေ့ရှိပါတယ်။

အာတူရိုဟာ ဆန္ဒပြပွဲတွေကို မြေပြင်မှာကိုယ်တိုင် ဦးဆောင်စီစဉ်သူဖြစ်ပြီး၊ အာဏာအလွဲသုံးစားမှုတွေကို မှတ်တမ်းတင်သူလည်းဖြစ်ပါတယ်။ သူဟာ သတင်းထောက်တွေ၊ အလုပ်သမားသမဝါယမအဖွဲ့တွေနဲ့ ဆက်သွယ် ပြောဆိုလေ့ရှိသလို၊ တစ်ခါတရံမှာတော့ သက်သေခံအချက်အလက် ဖော်ထုတ်တိုင်ကြားလိုသူတွေ ဒေသခံ တွေနဲ့လည်း အဆက်အသွယ်လုပ်လေ့ရှိပါတယ်။ ခြိမ်းခြောက်မှုပုံစံကို ပုံဖော်လေ့လာခြင်း (threat modelling) ရဲ့ ပထမဆုံးမေးခွန်းဖြစ်တဲ့"အာတူရို ဘာတွေကို ကာကွယ်ဖို့ကြိုးစားနေတာလဲ" ဆိုတာကို ဖြေကြည့်ကြပါစို့။ လူအခွင့်အရေးတက်ကြွလှုပ်ရှားသူတစ်ဦးအနေနဲ့ သူ့မှာ ကွန်ရက်ကြီးတစ်ခုရှိပါတယ်။ ဒါကြောင့် သူကာကွယ်ဖို့ ကြိုးစားနေတဲ့အရာတွေထဲမှာ တက်ကြွလှုပ်ရှားသူတွေရဲ့ ဆက်သွယ်ချိတ်ဆက်ဖို့လိုအပ်တဲ့ အချက်အလက်တွေ၊ သက်သေခံ အချက်အလက် ဖော်ထုတ်တိုင်ကြားလိုသူတွေ နဲ့ ပြောဆိုထားတဲ့ အချက်အလက်မှတ်တမ်းတွေနဲ့ မတရား နှိပ်စက် ညှင်းတာခံထားတာရမျိုး ၊ အာဏာအလွဲသုံးစားမှု တွေကို မှတ်တမ်းတင်ထားတဲ့ အရေးကြီးတဲ့ ဗီဒီယိုတွေ၊ ဓာတ်ပုံ တွေပါဝင်ပါတယ်။ လှုပ်ရှားမှုတွေပြုလုပ်နေစဉ်မှာ သူ မည်သူမည်ဝါဖြစ်ကြောင်းသိစေနိုင်တဲ့ ကိုယ်ပိုင်အချက်အလက်နဲ့ တည်နေရာကို လည်း သင့်လျော်မှန်ကန်တဲ့ နည်းလမ်းတစ်ခု ရှာဖွေအသုံးပြုကာကွယ်ဖို့ ထည့်သွင်းစဉ်းစားသင့်ပါတယ်။

ဒုတိယမေးခွန်းနဲ့ပတ်သတ်လို့ အာတူရိုလုပ်ကိုင်နေတဲ့ အလုပ်တွေရဲ့ အရေးကြီးထိလွယ်ရှလွယ်ဖြစ်မှုတွေကို ထည့်တွက်ကြည့် မယ်ဆိုရင် သူဟာ ဒေသခံအာဏာပိုင်တွေနဲ့ ရန်လိုတဲ့အဖွဲ့အစည်းတွေရဲ့ စောင့်ကြည့်မှုအောက်ကို ရောက်ရှိနိုင်ပါတယ်။ ဒီလိုစောင့်ကြည့်ခံရတဲ့အခါ အဲဒီအဖွဲ့တွေက ဥပဒေကို အသုံးပြုတာလည်းရှိသလို ဥပဒေမဲ့လုပ်ရပ်တွေ ကိုလည်း အသုံးပြုလာ နိုင်ပါတယ် ။အကယ်၍ အာတူရိုမှာ အင်တာနက်ဆိုရှယ်မီဒီယာအကောင့် ဒါမှမဟုတ် အင်တာနက်ကွန်ရက်တွေကို အသုံးပြုနေတယ် ဆိုရင်သူ့ကို အင်တာနက်ပေါ်မှာ ခြိမ်းခြောက်ဖို့ကြိုးစားနေတဲ့ နောက်ပြောင်ရန်စမှု (Trolls) တွေ ဒါမှမဟုတ် ပုဂ္ဂိုလ်ရေးဆိုင်ရာ အချက်အလက်တွေကို ခိုးယူပြီး အင်တာနက်ပေါ်မှာ ဖော်ထုတ်သူ တွေရဲ့ သားကောင် ဖြစ်လာနိုင်ပါတယ်။ လုံခြုံသောဆက်သွယ်ရေးမူဘောင် (SCF) အရ အရ အာတူရို ကိုင်တွယ်နေရတဲ့ အချက်အလက်အများစုဟာ လိမ္မော်ရောင် ဒါမှမဟုတ် အနီရောင် ဧရိယာတွေထဲမှာရှိနေပြီး အဲဒါတွေဟာ ပစ်မှတ်ထားခံရနိုင်ခြေအလွန်မြင့်မားတဲ့ အရေးကြီးထိလွယ်ရှလွယ်ဖြစ်တဲ့ အချက်အလက်တွေ ဖြစ်ပါတယ်။ သူဟာ သက်သေခံအချက်အလက် ဖော်ထုတ် တိုင်ကြားလိုသူတွေနဲ့ဆက်သွယ်မှုတွေ၊ အလွဲသုံးစားမှု တွေကို မှတ်တမ်းတင်ထားတဲ့ မီဒီယာအထောက်အထားတွေ၊ ဆန္ဒပြပွဲတွေ စီစဉ်တာတွေအပြင် အရေးကြီးတဲ့ ဆက်သွယ်ရန်အမည်စာရင်း တွေကို ကိုင်တွယ်နေရပါတယ်။ အဲဒီအချက်အလက်တွေ ပေါက်ကြားသွားရင် အသိုင်းအဝိုင်းနဲ့ လူ့အသက်တွေကိုပါ အန္တရာယ်ဖြစ်စေနိုင်ပါတယ်။ ဒါဆိုရင် အာတူရိုနဲ့ကြားခံ ဆက်စပ်သူတွေရဲ့ စွမ်းဆောင်ရည်နဲ့ ရည်ရွယ်ချက်ကကော ဘယ်လိုလဲ။ ဖိလစ်ပိုင်မှာ တက်ကြွလှုပ်ရှားသူတွေကို စောင့်ကြည့်တာ၊ နှောင့်ယှက်တာတွေလုပ်တဲ့ ဖြစ်စဉ်ဟာ သမိုင်းကြောင်းရှည်ကြာစွာရှိခဲ့ပါတယ်။ အဲဒီအတွက် အာတူရိုကြိုတွေ့ရမယ့် ခြိမ်းခြောက်မှုဟာ အမှန်တကယ်လက်တွေ့၊ ချက်ချင်းဆိုသလို ဖြစ်ပွားနိုင်ပါတယ်။ နိုင်ငံတွင်းက ဒေသခံဥပဒေစိုးမိုးရေးအဖွဲ့တွေဟာ ဆန္ဒပြပွဲစီစဉ်သူတွေရဲ့ လှုပ်ရှားမှုတွေ ခြေရာခံတာ၊ သူတို့ရဲ့ ဆက်သွယ်ပြောဆိုမှု တွေကို ကြားဖြတ်ဖမ်းယူနားထောင်တာ၊ တစ်ခါတရံမှာ ရှင်းရှင်းလင်းလင်းမရှိတဲ့ ဥပဒေ အကြောင်းပြချက်တွေနဲ့ ကြိုတင်ဖမ်းဆီးတာတွေ လုပ်လေ့ရှိတယ်လို့ လူသိများပါတယ်။ အဲဒီအချက်တွေကြောင့် အာတူရိုဟာ အရမ်းအန္တရာယ်များတဲ့ ပတ်ဝန်းကျင်မှာရှိနေပြီး သူ့ရဲ့ တတ်ကြွလှုပ်ရှားမှုလုပ်ငန်းတွေကို စောင့်ကြည့်ခံ ရတာနဲ့ ဟန့်တားခံရတာတွေဖြစ်လာနိုင်ဖို့ အလားအလာများပါတယ်။ ဒါကြောင့် သူ့ရဲ့အန္တရာယ်အဆင့်ကို အရေးကြီးတဲ့ အနီရောင်ဇုန် (critical red zone) မှာ ရှိတယ်လို့ အခိုင်အမာသတ်မှတ်နိုင်ပါတယ်။

ဒီလိုမျိုး အရေးကြီးတဲ့ အခြေအနေတွေမှာ ခြိမ်းခြောက်မှုတွေကလည်း ကြီးကြီးမားမားရှိနေတဲ့အတွက် အချက်အလက် တွေပေါက်ကြားမှုဖြစ်ခဲ့ရင် ကြောက်မက်ဖွယ်ကောင်းတဲ့ အကျိုးဆက်တွေ ဖြစ်လာနိုင်ပါတယ်။ အချက်အလက်တွေ ပေါက်ကြားခဲ့ရင် ပစ်မှတ်ထား နှောင့်ယှက်ခံရတာ၊ ဥပဒေမဲ့ဖမ်းဆီးခံရတာ၊ အတင်းအဓမ္မအစအနပျောက်ဆုံး သွားတာ မျိုးနှင့် တရားလက်လွတ် သတ်ဖြတ်ခံရတာတွေအထိ ဖြစ်ပေါ်လာနိုင်ပါတယ်။ သက်သေခံအချက်အလက် ဖော်ထုတ် တိုင်ကြားလိုသူတွေ ဒါမှမဟုတ် သတင်းပေးတွေရဲ့ မည်သူမည်ဝါဖြစ်ကြောင်း သိစေနိုင်တဲ့ သတင်းအချက် တွေ ပေါက်ကြားသွားတာမျိုးကလည်း တက်ကြွလှုပ်ရှားသူတွေရဲ့ကွန်ရက်တွေကို သိသိသာသာ ပျက်စီးစေနိုင်ပြီး ကိုယ့်ကိုယ်ကိုယ် ဆင်ဆာပြန်ဖျက်နေရတာမျိုးတွေလိုလက်တွေ့ဘဝအကျိုးဆက်တွေကို ဖြစ်ပေါ်စေနိုင်ပါတယ်။ အချက်အလက်ပေါက်ကြားမှုတစ်ခုဖြစ်သွားခဲ့ရင်

အာတူရိုရဲ့ တတ်ကြွလှုပ်ရှားမှုတွေကို ရပ်တန့်စေရုံသာမက ကွန်ရက် အတွင်းမှာရှိတဲ့ ယုံကြည်မှုကိုပါ ပျက်ပြားစေမယ်ဆိုတာကို ကျွန်တော်တို့ သေချာသိ နိုင်ပါတယ်။

ဒီအခြေအနေတွေကိုကြည့်ပြီး အာတူရိုနဲ့ သူ့ရဲ့လုပ်ဖော်ကိုင်ဖက် တက်ကြွလှုပ်ရှားသူတွေ ကိုယ့်ကိုယ်ကိုယ် ကာကွယ်နိုင် မယ့် နည်းလမ်းတချို့ကို အကြံပြုပေးသွားပါမယ်။ ပထမဆုံးအနေနဲ့ အာတူရိုအနေနဲ့ အရေးကြီး၊ထိလွယ်ရှလွယ်ဖြစ်တဲ့ စကားပြောဆိုဆက်သွယ်မှုတွေအတွက် အလုံးစုံစာဝှက်လျှို့ဝှက်ကုဒ်စနစ် သုံးစာပို့နည်း (E2EE encrypted messaging) ကို အသုံးပြုသင့်ပြီး သတ်မှတ်ချိန်ရောက်ရင် ဆက်သွယ်ပြောဆိုထားတဲ့ အချက်အလက်တွေကို အလိုအလျောက်ပယ်ပျက် ပေးတဲ့စာပို့စနစ် (self-deleting messages) ကို သုံးသင့်ပါတယ်။ ဒါ့အပြင် အရေးကြီးတဲ့ အထောက်အထားတွေကို လုံခြုံစွာ သိမ်းဆည်းနိုင်ဖို့အတွက် ၃-၂-၁-၁-၀ နည်းလမ်းကိုသုံးပြီး သိမ်းဆည်းထားဖို့ လိုအပ်နိုင်ပါတယ်။ ၃ က အချက်အလက်မိတ္တူ သုံးခုရှိဖို့၊ ၂ က မတူညီတဲ့ သိုလှောင်မှုပုံစံ နှစ်ခုနဲ့ သိမ်းဆည်းဖို့၊ ၁ က မိတ္တူ တစ်ခုကို အင်တာနက်ရဲ့ အပြင်ဘက်နေရာတစ်ခုမှာထားဖို့၊ နောက် ၁ က မိတ္တူ တစ်ခုကို ကွန်ရက်နဲ့ လုံးဝအဆက်အသွယ်မရှိတဲ့ အင်တာနက်ပြင်ဘက်နေရာတစ်ခုမှာထားဖို့ ၊ ၀ ကတော့ အထောက်အထားတွေ ကိုသိမ်းဆည်းတဲ့လုပ်ငန်းစဉ်မှာ လုံးဝအမှားအယွင်း မရှိစေဖို့ ဖြစ်ပါတယ်။

အာတူရိုဟာ သူ့ရဲ့အရေးကြီးတဲ့အင်တာနက်အကောင့်တွေအားလုံးအတွက် အချက်များစွာဖြင့် စစ်မှန်ကြောင်း အတည် ပြုခြင်း (multi-factor authentication) ကို သုံးစွဲဖို့ စဉ်းစားနိုင် ပါတယ်။ ဒါ့အပြင် ခိုင်မာ ပြီး တစ်မူထူးခြားတဲ့ အဓိက စကားဝှက် (master password) ကို လျှို့ဝှက်ဖုံးကွယ်ထားပေးနိုင်တဲ့ စကားဝှက်မန်နေဂျာ (password manager) ကိုလည်း တွဲဖက်အသုံးပြုနိုင်ပါတယ်။ သူရဲ့ဖုန်းကို ဖွင့်တဲ့အခါမှာလည်း မျက်နှာမှတ်သားသောစနစ် (facial recognition) ဒါမှမဟုတ် လက်ဗွေရာ (fingerprints) ကိုသုံးပြီးဖွင့်တဲ့စနစ်တွေကို ရှောင်ရှားတာက ပိုအကျိုးရှိနိုင်ပါ တယ်။ အကြောင်းကတော့ ဇီဝဆိုင်ရာ အချက်အလက်တွေသုံးတဲ့စနစ်တွေ (biometric methods) ဟာ သူရဲ့ခွင့်ပြုချက် မပါဘဲ အတင်းအကျပ် အသုံးပြု ခံရနိုင်လို့ပါပဲ။ အဲဒီအစား ခိုင်မာတဲ့ နံပါတ် (PIN) ဒါမှမဟုတ် လျှို့ဝှက် စာစု (passphrase) တွေကို အသုံးပြု နိုင်ပါတယ်။ လုံခြုံရေး ပိုမိုအားကောင်းစေဖို့၊ အထူးသဖြင့် နယ်စပ် ဖြတ်ကျော်ချိန် ဒါမှမဟုတ် သူရဲ့ ကိရိယာစက်ပစ္စည်း တွေကို သိမ်းဆည်းခံရနိုင်တဲ့ အန္တရာယ်ရှိတဲ့အခါမျိုးမှာ အာတူရို ဟာ သူရဲ့ ကိရိယာ စက်ပစ္စည်း များက လုံးဝပိတ်ထားဖို့ လိုအပ်နိုင်ပြီး ခရီးမသွားခင် အရေးကြီးပြီးထိလွယ်ရှလွယ်ဖြစ်စေနိုင်တဲ့ ဆက်သွယ် စာပို့တဲ့ အပလီကေးရှင်း (messaging apps) တွေကို ဖျက်ပစ်ဖို့ပါ စဉ်းစားသင့်ပါတယ်။ အချက်အလက်တွေ မတော်တဆပေါက်ကြားမှု အန္တရာယ်ကို လျော့ချနိုင်ဖို့အတွက် အာတူရိုဟာ ခွင့်ပြုချက်မရှိဘဲ အသံနဲ့ ထိန်းချုပ်အသုံးပြု တာတွေကို တားဆီးနိုင်ဖို့အတွက် ဖုန်းကိုပိတ်ထားစဉ်မှာ အသံကိုအသုံးပြုပြီးစေခိုင်းသောစနစ်(voice assistants) တွေကို ပိတ်ထားဖို့ လိုအပ်နိုင်ပါတယ်။ ဒါ့အပြင် သူရိုက်ကူးထားတဲ့ ဓာတ်ပုံနဲ့ ဗီဒီယိုတွေမှာပါတဲ့ EXIF နောက်ဆက်တွဲအချက်အလက် (EXIF metadata) တွေကို ဖယ်ရှားပြီးမှ မျှဝေတာမျိုးလုပ်ဖို့ လိုအပ်ပါတယ်။ အကြောင်းကတော့ ဓာတ်ပုံတွေထဲမှာပါတဲ့ တည်နေရာ အချက် အလက်တွေက အရေးကြီးပြီး ထိလွယ်ရှလွယ် ဖြစ်တဲ့ နေရာတွေကို မတော်တဆ ဖော်ထုတ်ပေးနိုင်တာကြောင့်ပါ။ နောက်ဆုံးအနေနဲ့ အာတူရိုဟာ အန္တရာယ်အရမ်းများ

စေတဲ့အစည်းအဝေးတွေ ဒါမှမဟုတ် အရေးကြီးပြီး ထိလွယ်ရှလွယ်ဖြစ်စ နိုင်တဲ့ အလုပ်တွေ လုပ် နေချိန်မှာ ဘလူးတူ (Bluetooth) နားကြပ်တွေနဲ့ စမတ်နာရီ (Smartwatches) တွေလို မျိုးကြိုးမဲ့ပစ္စည်းကိရိယာတွေကို အသုံးပြု တာမျိုး ရှောင်သင့်ပါတယ်။

အာတူရိုရင်ဆိုင်နေရတဲ့ ခြိမ်းခြောက်မှုဆိုင်ရာ ပုံစံကို လေ့လာနားလည်းခြင်းက သူဘာတွေလိုအပ်တယ်၊ ဘယ်သူတွေက သူ့ကို ပစ်မှတ်ထားနေတယ်၊ သူဘာတွေလုပ်နိုင်တယ်ဆိုတာနဲ့ပတ်သတ်ပြီး ရှင်းလင်းတဲ့လုပ်ငန်းစဉ် ချမှတ်နိုင်ဖို့ အထောက်အကူပြုပါတယ်။ ပြီးပြည့်စုံတဲ့ ဒစ်ဂျစ်တယ်လုံခြုံရေးနည်းဗျူဟာကို ရှာဖွေတာဟာ လူအများအတွက် ခက်ခဲနိုင်ပါတယ်။ ဘာကြောင့်လဲ ဆိုတော့ အထူးသဖြင့် ရွေးချယ်စရာတွေနဲ့ နည်းလမ်းတွေ အများကြီးရှိလို့ပါပဲ။ ဒါပေမဲ့ လိုအပ်ချက်တွေ၊ စွမ်းဆောင်ရည်တွေနဲ့ ဖြစ်နိုင်ခြေတွေကို အခြေခံပြီး ခွဲခြမ်းစိတ်ဖြာခြင်းအားဖြင့် ရှုပ်ထွေးလွန်းတဲ့ လုပ်ငန်းစဉ်ကြောင့် ဘာမှမလုပ်နိုင်ဘဲ ဖြစ်မနေဘဲ အချက်အလက် အခြေခံတဲ့ ဆုံးဖြတ်ချက်တွေကို ချမှတ်နိုင်ပါတယ်။

နောက်ဆက်တွဲအချက်အလက်များ (Metadata) များ အကြောင်း ကို နားလည်ခြင်း

ယခင်အပိုင်းမှာ ဓာတ်ပုံတွေကို မျှဝေခြင်းမပြုခင် EXIF အချက်အလက်တွေကို ဖယ်ရှားပစ်ဖို့ အကြံပြုခဲ့ပါတယ်။ EXIF ဆိုတာက လွှဲပြောင်းပေးပို့နိုင်တဲ့ ဓါတ်ပုံဖိုင်ရဲ့ ပုံစံ (Exchangeable image file format) ရဲ့ အတိုကောက်ဖြစ်ပြီး၊ ဒါဟာ နောက်ဆက်တွဲအချက်အလက် (Metadata) တစ်မျိုးပါ[26]။ နောက်ဆက်တွဲ အချက်အလက်များ (Metadata) ဆိုတာကတော့ "အချက်အလက်တွေနဲ့ပတ်သက်တဲ့ အချက်အလက်" လို့ အဓိပ္ပါယ်ရပါတယ်။ ဒါဟာ ဖိုင်တွေ၊ ဆက်သွယ်ပြောဆိုထားတဲ့စာတွေနဲ့ ဒစ်ဂျစ်တယ်လှုပ်ရှားမှုတွေမှာ ပါဝင်နေတဲ့ နောက်ခံအချက်အလက်တွေဖြစ်ပြီး ဘယ်လို၊ ဘယ်အချိန်၊ ဘယ်နေရာနဲ့ ဘယ်သူက ဘယ်အရာကို လုပ်ခဲ့တယ်ဆိုတာမျိုးကို ဖော်ပြပေးပါတယ်။ ဥပမာအနေနဲ့ ထိုင်းနိုင်ငံကို ခဏတာသွားရောက်လည်ပတ်စဉ်က ရိုက်ခဲ့တဲ့ ဒီပုံဟောင်းကို ကြည့်နိုင်ပါတယ်။

[26] Chester Avey, “What to Know About EXIF Data, a More Subtle Cybersecurity Risk,” *ISACA*, February 6, 2025, https://www.isaca.org/resources/news-and-trends/industry-news/2025/what-to-know-about-exif-data-a-more-subtle-cybersecurity-risk

File:MIMEType	"image/jpeg"
File:ExifByteOrder	"Big-endian (Motorola, MM)"
File:ImageWidth	767
File:ImageHeight	1366
File:EncodingProcess	"Baseline DCT, Huffman coding"
File:BitsPerSample	8
File:ColorComponents	3
File:YCbCrSubSampling	"YCbCr4:2:0 (2 2)"
JFIF:JFIFVersion	1.01
JFIF:ResolutionUnit	"inches"
JFIF:XResolution	96
JFIF:YResolution	96
EXIF:GPSVersionID	"2.2.0.0"
EXIF:GPSLatitudeRef	"North"
EXIF:GPSLatitude	13.7940141666667
EXIF:GPSLongitudeRef	"East"
EXIF:GPSLongitude	100.321111111111
EXIF:GPSAltitudeRef	"Above Sea Level"
EXIF:GPSAltitude	17.5
EXIF:GPSMeasureMode	"3-Dimensional Measurement"
EXIF:GPSDOP	1208
EXIF:Padding	{ "_ctor": "BinaryField", "bytes": 4108, "rawValue": "(Binary data 4108 bytes, use -b option to extract)" }
Composite:ImageSize	"767×1366"
Composite:Megapixels	1
Composite:GPSAltitude	17.5
Composite:GPSLatitude	13.7940141666667
Composite:GPSLongitude	100.321111111111
Composite:GPSPosition	"13.7940141666667 100.321111111111"

ဓာတ်ပုံရှင်းလင်းချက်- ဤပုံသည် JPEG ဖိုင်တစ်ခု၏ ပုံရဲ့အချက်အလက်တွေနဲ့ ပတ်သတ်ပြီးဖော်ပြတဲ့ နောက်ဆက်တွဲအချက်အလက် (Metadata)ကို ဖော်ပြထားသော ဖန်သားပြင်ပုံ ဖြစ်သည်။ ၎င်းတွင် နေရာပြစနစ် (GPS) ၏ တည်နေရာများ၊ ပုံ၏ အရွယ်အစားနှင့် ကုဒ်သွင်းပုံစံ၊ ပုံ၏ ကြည်လင်ပြတ်သားမှုနှင့် အရောင်အစိတ်အပိုင်းများကဲ့သို့သော နည်းပညာဆိုင်ရာ အချက်အလက်များ ပါဝင်သည်။

ပုံမှာပြထားတဲ့အချက်အလက်တွေမှာ ဓာတ်ပုံရဲ့ ရုပ်ထွက်အရည်အသွေး (resolution)၊ ဘယ်ဖုန်းနဲ့ရိုက်ကူးခဲ့လဲ၊ ပုံရဲ့အရွယ်အစား၊ ဘယ်အချိန်က ရိုက်ခဲ့တာလ` (အခုပြထားတဲ့ပုံမှာတော့ မပါဝင်ပါဘူး) နဲ့ တည်နေရာတွေ (Global Positioning System) ပါဝင်နေပါတယ်။ ဒီလိုမျိုး မမြင်နိုင်တဲ့ အချက်အလက်တွေဟာ သင် ဘယ်လို အကြောင်းအရာ တွေကို ဆက်သွယ် ဆက်သွယ်ပြောဆိုနေတယ်ဆိုတာကို ဘယ်သူမှ မသိရင်တောင်မှ သင့်ရဲ့ အင်တာနက်ကွန်ရက်၊ သင့်ရဲ့ပုံမှန်သွားလာလှုပ်ရှားမှုပုံစံ ဒါမှမဟုတ် သင့်ရဲ့တည်နေရာ ကို ဖော်ထုတ်ဖို့ လုံလောက်ပါတယ်။ တက်ကြွလှုပ်ရှား သူတွေအနေနဲ့ လူ့အခွင့်အရေးချိုးဖောက်မှုတွေကို မှတ်တမ်း တင်ထားတဲ့ ဓာတ်ပုံ တွေကို အရေးကြီးတဲ့ အချက်အလက် (EXIF) နဲ့အတူ မျှဝေလိုက်မိရင် အဲဒီအချက်အလက်တွေကို ရိုက်ကူးခဲ့တဲ့သူ ဒါမှမဟုတ် အမည်မဖော်လိုတဲ့ သက်သေ လိုက်ပေးတဲ့ သူတွေကို အာဏာပိုင်တွေက တိုက်ရိုက် ခြေရာ ခံနိုင်ပါတယ်။

သတင်းထောက်တွေနဲ့ မျှဝေတဲ့ စာရွက်စာတမ်းတွေ၊ စာရင်းဇယားတွေ (Spreadsheets) ဒါမှမဟုတ် PDF ဖိုင် တွေမှာလည်း တူညီတဲ့အန္တရာယ်ဟာအလားအလာရှိပါတယ်။ စာဝှက်လျှို့ဝှက်ကုဒ်စနစ်သုံးအီးမေး (encrypted emails) တွေမှာလည်း နောက်ဆက်တွဲအချက်အလက် (Metadata) တွေပါဝင် နေနိုင်ပါတယ်။ ဘာကြောင့်လဲဆိုတော့ သင့်ကိုအီးမေး ဝန်ဆောင်မှုပေးတဲ့သူတွေက အီးမေးလ်ကို ဘယ်နေရာကို ပို့ပေး ရမလဲဆိုတာ သူတို့ သိဖို့ လိုအပ်တာကြောင့်ပါ။ နောက်ဆက်တွဲအချက်အလက်များ (Metadata) ဟာ လူတွေရဲ့ ကိုယ်ရေး

အချက်အလက် တွေကို စုဆောင်း တည် ဆောက် ရာအတွက် ဂိတ်တံခါးတစ်ခုဖြစ်ပြီး ဒါကို ကွန်ယက်မြေပုံ တည်ဆောက်ခြင်း (network mapping) လို့ခေါ်ပါတယ်။ ကို ကွန်ယက်မြေပုံ (network maps) တွေဟာ နောက်ဆက်တွဲအချက်အလက် (Metadata) တစ်ခုတည်းကနေပဲ သင့်ရဲ့ လူမှုကွန်ယက်ဆက်ဆံရေးနမူနာပုံစံ (social graphs) တွေကို ပြန်လည်တည်ဆောက်နိုင်ပါတယ်။ ဒါဟာ သင်ဘယ်သူနဲ့ ဆက်သွယ်စာပို့နေလဲ၊ အကြိမ်ဘယ်လောက် ပို့နေလဲဆိုတာကိုပါ ခြေရာခံနိုင်ပါတယ်။ ဥပမာအနေနဲ့ အိန္ဒိယနိုင်ငံမှာ ဥပဒေစိုးမိုးရေး ဌာနတွေဟာ နေ့စဉ်ဖြစ်ရိုးဖြစ်စဉ်ကိစ္စတွေနဲ့ ရာဇဝတ်မှုတွေကို စုံစမ်းစစ်ဆေးဖို့အတွက် နောက်ဆက်တွဲ အချက်အလက် (Metadata) တွေကို အသုံးပြုနေကြပါတယ်။ အကြောင်းအရာတွေကို ဝင်ရောက်ကြည့်ရှုတာ မျိုး မလုပ်ဘဲ အသေးစိတ်ကျတဲ့ အပြုအမူဆိုင်ရာ အချက်အလက်တွေကို တည်ဆောက်ဖို့ ခေါ်ဆိုမှုမှတ်တမ်း တွေကို ခြေရာခံတာ၊ အသုံးပြုတဲ့ စက် တွေကို ဖော်ထုတ်တာ၊ အိုင်ပီလိပ်စာ (IP) တွေကို စောင့်ကြည့်တာ၊ ပြီးတော့ တည်နေရာအချက်အလက်တွေကို ခွဲခြမ်းစိတ်ဖြာတာ မျိုးတွေ လုပ်ဆောင်ပါတယ်[27]။ တခြားနိုင်ငံတွေမှာတော့ ဒီလိုလုပ်ပိုင်ခွင့်ကို အလွဲသုံးစားလုပ်ခဲ့ကြပါတယ်။ ဥပမာအနေနဲ့ ဩစတြေးလျရဲတပ်ဖွဲ့ဟာ သတင်းထောက်တစ်ဦးရဲ့ ဖုန်းထဲကနေ နောက်ဆက်တွဲအချက်အလက် (Metadata) တွေကို တရားမဝင်ရှာဖွေခဲ့တယ်လို့ တွေ့ရှိခဲ့ပါတယ်[28]။ဒါက ဒီလိုအလွဲသုံးစားမလုပ်နိုင်အောင် တရားဝင်ကြီးကြပ်မှု စနစ်တွေရှိတဲ့ နိုင်ငံတွေမှာတောင် နောက်ဆက်တွဲအချက် အလက် (Metadata) တွေကို ဘယ်လောက်လွယ်လွယ်ကူကူ အလွဲသုံးစားလုပ် နိုင်လဲဆိုတာကို ပြသနေ ပါတယ်။

နောက်ဆက်တွဲအချက်အလက် (Metadata) စောင့်ကြည့်ခြင်းဟာ ပစ်မှတ်ထားအွန်လိုင်းလှည့်စားမှု (targeted phishing) တိုက်ခိုက်မှုတွေလိုမျိုး ပိုမိုဆိုးရွားတဲ့ တိုက်ခိုက်မှုတွေအတွက်လည်း လမ်းဖွင့်ပေးပါတယ်။ အကယ်၍ သူတို့က သင်ဟာ လူတစ်ယောက်နဲ့ အကြိမ်ရေဘယ်လောက်များများ ဆက်သွယ်စာပို့ပို့လဲဆိုတာကို သိရင် သင့်ရဲ့စနစ်ကို ဝင်ရောက်ဖို့အတွက် ပိုပြီးရှုပ်ထွေးတဲ့ အွန်လိုင်းလှည့်စားမှု (phishing) တိုက်ခိုက်မှုတွေကို အလွယ်တကူ ဖန်တီးနိုင်ပါတယ်။ သင့်နဲ့ပတ်သတ်တဲ့ နောက်ဆက်တွဲအချက်အလက် (Metadata) များများရရှိလေလေ၊ သူတို့ရဲ့တိုက်ခိုက်မှုဟာ ပိုပြီး ယုံကြည်စိတ်ချနိုင်အောင် ပုံဖော်နိုင်လေလေ ဖြစ်တယ်ဆိုတာကို သတိရပါ။

လုပ်ငန်းလည်ပတ်မှု လုံခြုံရေး (OPSEC) ဆိုတာဘာလဲ

၂၀၂၅ ခုနှစ်၊ မတ်လတုန်းက ဒစ်ဂျစ်တယ်လုံခြုံရေးကမ္ဘာကို တုန်လှုပ်စေခဲ့တဲ့ စစ်ဂနယ်တံခါးပေါက် (Signal Gate) ဖြစ်ရပ်ကို သင်မှတ်မိဦးမယ်ဆိုရင်၊ ဒါဟာ လုပ်ငန်းလည်ပတ်မှု လုံခြုံရေး (OPSEC) ဆိုင်ရာ ကျရှုံးမှုရဲ့ စံ

[27] Saravasti NT, “How India’s Police Is Using Metadata,” *Medianama*, November 23, 2023, https://www.medianama.com/2023/11/223-india-police-metadata-use-tracking-2/

[28] Matthew Doran and Henry Belot, “Australian Federal Police accessed journalists' metadata, stoking new media freedom concerns,” *ABC*, July 09, 2019, https://www.abc.net.au/news/2019-07-09/afp-access-journalist-metadata-60-times-in-12-months/11290888

နမူနာတစ်ခု ဖြစ်ပြီး သတင်းစာမျက်နှာတွေရဲ့ ရှေ့ဆုံးကို ရောက်ရှိခဲ့ပါတယ်[29]။ ဒီအဖြစ်အပျက်မှာ အမေရိကန် စစ်ဘက်အရာရှိတွေရဲ့ စစ်ဂနယ် အပလီကေးရှင်းရဲ့ စုဖွဲ့ဆွေးနွေးနိုင်တဲ့ ကွန်ယက် (Signal group chat) တစ်ခုထဲကို သတင်းထောက်တစ်ဦး မတော်တဆ ပါဝင်သွားခဲ့ပြီး အဲဒီ ဆက်သွယ်စာပို့တဲ့အစုအဖွဲ့ထဲမှာ ယီမင်နိုင်ငံကို တိုက်ခိုက်မယ့် စစ်ရေးအစီအစဉ် တွေကို ဆွေးနွေးနေခဲ့ကြတာပါ။ ဒီရှုပ်ထွေးမှုကြီးတစ်ခုလုံးနဲ့ပတ်သက်ပြီး မီဒီယာရဲ့အာရုံစိုက်မှုက စိတ်ပျက်စရာကောင်း ခဲ့ပါတယ်။ ဘာကြောင့်လဲဆို တော့ သူတို့ဟာ Jeffrey Goldberg ကို စစ်ဂနယ် အပလီကေးရှင်းရဲ့ စုဖွဲ့ ဆွေးနွေးနိုင်တဲ့ ကွန်ယက် ထဲကို ထည့်မိတဲ့ အမှားအယွင်းအပေါ်မှာပဲ အာရုံစိုက်ခဲ့ကြပြီး "ယီမင်ကို ဘာကြောင့် ထပ်ပြီး ဗုံးကြဲနေရ တာလဲ"၊ "ဒီစစ်ပွဲတွေကနေ ဘယ်သူတွေ အကျိုးအမြတ်ရနေလဲ"၊ "လက်နက်တွေ ဘယ်သူတွေက ထောက်ပံ့နေတာလဲ" ဆိုတဲ့ မေးခွန်းတွေကိုတော့ မေးခွန်းထုတ်ခဲ့ခြင်း မရှိလို့ပါပဲ။

ဒီဖြစ်ရပ်က လုပ်ငန်းလည်ပတ်မှု လုံခြုံရေး (OPSEC) နဲ့ပတ်သက်ပြီး အရေးကြီးတဲ့အချက်တစ်ခုကို ဖော်ထုတ်ပြသနေပါတယ်။ ဒါဟာ နည်းပညာပိုင်းဆိုင်ရာ ချွတ်ယွင်းချက်တစ်ခုထက် ပိုကြီးတဲ့အရာတစ်ခုကို ပြသနေတာပါ။ အဲဒါကတော့ အင်အားကြီးမားတဲ့သူတွေတောင် တကယ်ကို ပေါ့ဆနိုင်တယ်ဆိုတာကို ကျွန်တော်တို့ကို သတိပေး နေတာပါ။ လူတိုင်းဟာ လူသားတွေဖြစ်တဲ့အတွက်အမှားတွေကနေ ကင်းလွတ်ကြတာမဟုတ်ပါဘူး။ ဒါ့အပြင် ဘယ် လောက်ကောင်းတဲ့ နည်းပညာဖြစ်ဖြစ် အရေးကြီးပြီးထိလွယ်ရှလွယ်ဖြစ်တဲ့အချက်အလက်တွေကို ကိုင်တွယ်ရာမှာ စည်းကမ်းရှိမှုနဲ့ ရည်ရွယ်ချက်ရှိရှိ လုပ်ဆောင်မှုကို အပြည့်အဝ အစားထိုးနိုင်မှာ မဟုတ်ပါဘူး (ကံမကောင်းစွာနဲ့ စစ်ရာဇဝတ်မှုတွေလည်း အပါအဝင်ပါပဲ)။ လုပ်ငန်းလည်ပတ်မှု လုံခြုံရေး (OPSEC) ဆိုတာက Operational Security ရဲ့ အတိုကောက်ဖြစ်ပါတယ်။ ဒါဟာ သင့်မှာ ဘယ်လိုအချက်အလက်တွေရှိလဲ၊ အဲဒီအချက်အလက်တွေကို ဘယ်လိုရှာဖွေတွေ့ရှိနိုင်မလဲ၊ အန္တရာယ် အလားအလာကို လျှော့ချဖို့ ဘယ်လို လုပ်ဆောင်ချက်တွေ လုပ်နိုင်မလဲဆိုတာတွေကို ဖော်ထုတ်တဲ့ လုပ်ငန်းစဉ်တစ်ခု ဖြစ်ပါတယ်။ လုပ်ငန်းလည်ပတ်မှု လုံခြုံရေး (OPSEC) ဟာ နည်းပညာပိုင်းဆိုင်ရာသက်သက်မဟုတ်ဘဲ အတွေးအခေါ်ပိုင်းဆိုင်ရာ (တည်ရှိမှုဆိုင်ရာ) ပိုပြီးဆန်ပါတယ်။ ဘာကြောင့်လဲဆိုတော့ အကောင်းဆုံးမေးခွန်းတွေ မေးဖို့လိုတာကြောင့်ပါ။ ဥပမာသင်က ခရီးသွားမယ့်အစီအစဉ်တွေကို စုဖွဲ့ဆွေးနွေးနိုင်တဲ့ကွန်ယက် (group chat) ထဲမှာ ပေါ့ပေါ့ပါးပါး ပြောနေမိသလား။ သင့်ရဲ့ အင်တာနက် အကောင့် တွေက သင့်ကိုမည်သူမယ်ဝါဖြစ်ကြောင်း ဖော်ထုတ်နိုင်တဲ့ ကိုယ်ပိုင်အချက်အလက်တွေကို ဖော်ထုတ်နိုင်စေတဲ့နည်းလမ်းတွေနဲ့ ချိတ်ဆက်ထားသလား။ သင့်ရဲ့ ပုံမှန် လုပ်ဆောင်နေကျ အရာတွေဟာ ကြိုတင်ခန့်မှန်းနိုင်လောက်အောင် လွယ်နေသလား (ဥပမာ- တွေ့ဆုံတဲ့နေရာ၊ အချိန်တွေ တူနေတာမျိုး)။ သင့်ရဲ့အင်တာနက်လူမှုမီဒီယာပို့စ်တွေက သင်ထင်တာထက် ပိုပြီးအချက်အလက်တွေ ပေးနေသလား။ ဒီမေးခွန်းတွေက ရန်လိုတဲ့အဖွဲ့အစည်းတွေအမြတ်ထုတ်နိုင်တဲ့ အားနည်းချက်တွေအဖြစ် ပြောင်းလဲသွား စေနိုင်တဲ့ လစ်ဟင်းချက်တွေကို ဖော်ထုတ်ပေးနိုင်ပါတယ်။

[29] Jeffrey Goldberg and Shane Harris, “Here are the attack plans that Trump’s advisers shared on Signal,” *The Atlantic*, March 25, 2025, https://www.theatlantic.com/politics/archive/2025/03/signal-group-chat-attack-plans-hegseth-goldberg/682176/

ကောင်းမွန်တဲ့ လုပ်ငန်းလည်ပတ်မှု လုံခြုံရေး (OPSEC) ဆိုတာ လူတိုင်းအတွက် မတူညီနိုင်ပါဘူး။ ခြိမ်းခြောက်မှုပုံစံ (Threat modelling) လိုပဲ ကောင်းမွန်တဲ့ လုပ်ငန်းလည်ပတ်မှု လုံခြုံရေး (OPSEC) ဟာလည်း နည်းဗျူဟာပုံစံ တစ်မျိုးဟာ လူတိုင်းအတွက် အဆင်ပြေစေမယ့် အရာမျိုးမဟုတ်ပါဘူး။ ဒါကြောင့် ဒစ်ဂျစ်တယ်ဆက်သွယ်မှုတွေ အားလုံးကို စောင့်ကြည့်နိုင်တယ်လို့ ယူဆထားဖို့နဲ့ သေးငယ်တဲ့ အချက်အလက်လေးအပိုင်းအစလေးတွေစုပေါင်းပြီး ပိုပြီးကြီးမားပြည့်စုံတဲ့ ပုံတစ်ပုံဖြစ်သွားနိုင်တယ်ဆိုတာကို နားလည်ထားဖို့က အရမ်းအရေးကြီးပါတယ်။သင့်ရဲ့ ကိုယ်ပိုင် ကောင်းမွန်တဲ့ လုပ်ငန်းလည်ပတ်မှု လုံခြုံရေး (OPSEC) ကို ကောင်းကောင်းမွန်မွန် အသုံးမချနိုင်ဘူး ဆိုရင် ဘယ်ကိရိယာမဆို အလုပ်ဖြစ်မှာမဟုတ်ပါဘူး။ ကောင်းမွန်တဲ့ လုပ်ငန်းလည်ပတ်မှု လုံခြုံရေး (OPSEC) ဟာ စည်းလုံးညီညွတ်မှုတစ်ရပ်ဖြစ်ပါတယ်။ ဒါဟာ သင့်ကိုယ်သင် ကာကွယ်ရုံသာမက သင်ဂရုစိုက်တဲ့သူတွေနဲ့ ကျနော်တို့ ပါဝင်နေတဲ့ တတ်ကြွလှုပ်ရှားမှုကိုပါ ကာကွယ်ပေးနိုင်တဲ့ နည်းလမ်းတစ်ခုဖြစ်ပါတယ်။

ဒုတိယပိုင်း- အဖြစ်များတဲ့ ခြိမ်းခြောက်မှုတွေနဲ့ တုံ့ပြန်နည်းဗျူဟာများ

ဆင်ဆာဖြတ်တောက်ခြင်းနှင့် ရှောင်ကွင်းခြင်း

ဆင်ဆာဖြတ်တောက်မှုဆိုတာ အချိန်ကာလကြာရှည်စွာကတည်းက တည်ရှိနေတဲ့ အရာတစ်ခုပါ။ ကမ္ဘာတစ်ဝန်းက အစိုးရတွေနဲ့ အုပ်ချုပ်ရေးအဖွဲ့အစည်းတွေအားလုံးနီးပါးဟာ အစိုးရအတိုက်အခံတွေကနေ သူတို့ကိုယ်သူတို့ ကာကွယ်ဖို့အတွက် ဒီနည်းလမ်းကို အသုံးပြုခဲ့ကြပါတယ်။ ရောမတွေလည်း ဆင်တာဖြတ်တောက်တာ လုပ်ခဲ့တယ်၊ အီဂျစ်တွေကလည်း ဆင်တာဖြတ်တောက်တာ လုပ်ခဲ့တယ်။ အခုခေတ်မှာတော့ နည်းဗျူဟာတွေက သိသိသာသာ အဆင့်ဆင့် ပြောင်းလဲလာခဲ့ပေမဲ့ ရည်ရွယ်ချက်ကတော့ အတူတူပဲဖြစ်ပါတယ်။ တာဝန်ယူမှု၊ တာဝန်ခံမှုတွေမရှိဘဲ အာဏာဆက်လက် ဆုပ်ကိုင်ထားဖို့ပဲဖြစ်ပါတယ်။ ဆင်ဆာဖြတ်တောက်မှုဟာ လစ်ဘရယ် ဒီမိုကရေစီ အမည်တပ်ထား တဲ့ နိုင်ငံတွေမှာလည်း ပိုပြီးဖော်ရွေ နူးညံ့တဲ့ပုံစံနဲ့ ရှင်သန်အသက်ဝင်နေပါတယ်[30]။ ဥပမာအနေနဲ့ ပါလက်စတိုင်းမှာ တရားမဝင်ကျူးကျော်သိမ်းပိုက်မှုတွေနဲ့ လူမျိုးတုံးသတ်ဖြတ်မှုတွေနဲ့ ပတ်သက်တဲ့ ပြောဆိုဆွေးနွေးမှုတွေဟာ မျက်မှောက်ခေတ်ဆင်ဆာဖြတ်တောက်မှုရဲ့ စံနမူနာပြယုဂ်တစ်ခုဖြစ်လာခဲ့ပြီး ပါလက်စတိုင်း လူမျိုးတွေရဲ့ အသံတွေကို အင်တာနက်လှုမှုကွန်ယက်မီဒီယာပလက်ဖောင်းများစွာမှာ ဆင်ဆာဖြတ်တောက်ခြင်းခံနေ ရပါတယ်[31]။ လူမှုကွန်ယက် မီဒီယာကုမ္ပဏီကြီးဖြစ်တဲ့ Meta (Facebook) ကတော့ အဲဒီ ဆင်ဆာဖြတ်တောက်မှုတွေကို သုံးစွဲသူများလိုက်နာရန် လမ်းညွှန်ချက်များ (community guidelines) ဆိုတဲ့ အကြောင်းပြချက်ကိုသုံးပြီး ပါလက်စတိုင်းတွေရဲ့ အခက်အခဲတွေ ကြား ရုန်းကန်လှုပ်ရှားမှု အကြောင်းအရာတွေ၊ ဇာတ်ကြောင်းတွေ လူသိရှင်ကြား ဖြုတ်ချနေပါတယ်[32]။ ကမ္ဘာကြီးကို ဆက်သွယ်ပေးဖို့ ရည်ရွယ်ပြီး ဒီဇိုင်းဆွဲထားတဲ့ ကိရိယာတွေကို လက်နက်သဖွယ် အသုံးပြုပြီးတော့ ဖိနှိပ်ခံလူတွေအကြောင်းကို မမြင်ရအောင် ဖုံးဖိထားကြပါတယ်။

---

30 Vasilis Ververis, “Internet censorship in the European Union” (PhD thesis, School of Business and Economics of Humboldt-Universität zu Berlin, 2022), https://edoc.hu-berlin.de/server/api/core/bitstreams/1d147948-861e-4a1f-9baf-b81bc786f06a/content.

31 Human Rights Watch, *Meta’s broken promise: Systemic censorship of Palestine content on Instagram and Facebook* (Human Rights Watch, 2023), https://www.hrw.org/report/2023/12/21/metas-broken-promises/systemic-censorship-palestine-content-instagram-and.

32 Sam Biddle, “Facebook Report concludes Company censorship violated Palestinian Human Rights,” *The Intercept*, September 21, 2022, https://theintercept.com/2022/09/21/facebook-censorship-palestine-israel-algorithm/

ဆင်ဆာဖြတ်တောက်မှုကို တိုက်ထုတ်ဖို့ဆိုတာ အင်တာနက်လူမှုကွန်ယက်စာမျက်နှာတွေမှာ ကျယ်ကျယ်လောင်လောင် နဲ့ အကြိမ်ရေများစွာ ဝေဖန်ပြောဆိုတဲ့အကြောင်းရေး တင်တာလောက်နဲ့ မပြီးပါဘူး။ အင်တာနက်ရဲ့ ဖွဲ့စည်းပုံကို နားလည်ဖို့နဲ့ ဆင်ဆာလုပ်နေတဲ့သူတွေအပေါ် မူတည်ပြီး ခြိမ်းခြောက်မှုပုံစံတွေက ပြောင်းလဲသွားနိုင်တယ်ဆိုတာကို အသိအမှတ်ပြုဖို့ လိုအပ်ပါတယ်။ ဆင်ဆာဖြတ်တောက်တာဟာ အစိုးရလား။ အင်တာနက်ဝန်ဆောင်မှုပေးသူ (ISP) လား။ ဒါမှမဟုတ် သင့်ကိုယ်သင် ပြန်ပြီး ဆင်ဆာဖြတ်တောက်သလို လုပ်တဲ့ပုံစံမျိုးလား။ ဒီအရာတွေအားလုံးထက် ပိုအရေးကြီးတာကတော့ နေရာ တော်တော်များများ မှာ နာခံမှုမရှိရင် ထောင်ချခံရတာ၊ နှောင့်ယှက်ခံရတာနဲ့ သေဆုံးတာ မျိုးတောင် ဖြစ်နိုင်တယ်ဆိုတဲ့ ခါးသီးတဲ့အမှန်တရားကို လက်ခံဖို့ပါပဲ။ ကံမကောင်းစွာနဲ့ ကျွန်တော်တို့ အများစုအတွက် ဆင်ဆာဖြတ်တောက်မှုကို တိုက်ထုတ်ဖို့ဆိုတာ နောက်ထပ် ကယ်ပေါက်/လွတ်ပေါက်တစ်ခု (loophole) ကို ရှာဖွေတာနဲ့တူနေပါတော့တယ်။

ဒီကယ်ပေါက်/လွတ်ပေါက်တွေဟာ အင်တာနက်ရဲ့ အလွှာအသီးသီးမှာ တည်ရှိနေတတ်ပြီး ဆင်ဆာဖြတ်တောက်မှုက လည်း ပုံစံအမျိုးမျိုး ရှိနိုင်ပါတယ်။ ဆင်ဆာဖြတ်တောက်မှု ကို အိုင်ပီလိပ်စာ (IP) ပိတ်ဆို့တာ၊ အင်တာနက်စာမျက်နှာ (website) အမည်များကို အိုင်ပီလိပ်စာ (IP) များအဖြစ် ပြောင်းလဲပေးသည့် လုပ်ငန်းစဉ် (DNS) ကိုပိတ်ဆို့တာ၊ အချို့သောအင်တာနက်တွင်ရရှိနိုင်သော ဝန်ဆောင်မှုများကို ပိတ်ဆို့တာနဲ့ အဆိုးဆုံးပုံစံဖြစ်တဲ့ အင်တာနက်ကွန်ယက် လုံးဝဖြတ်တောက်တာ (Internet blackout/shutdown) တွေနဲ့ လုပ်ဆောင်နိုင်ပါတယ်။

ဇယားနံပါတ် (၂)- ဆင်ဆာဖြတ်တောက်ရာတွင် အသုံးများသော နည်းလမ်းများ

ဆင်ဆာဖြတ်တောက်သောနည်း လမ်းများ	**ဖော်ပြချက်**
အိုင်ပီလိပ်စာ (IP) ပိတ်ဆို့ခြင်း	အင်တာနက်ဝန်ဆောင်မှုပေးတဲ့သူတွေ (ISP) က (အစိုးရရဲ့တိုက်ရိုက်အမိန့်နဲ့ပဲဖြစ်ဖြစ်) အိုင်ပီလိပ်စာ (IP) ပိတ်ဆို့မှုတွေကို အသုံးပြုပြီး ချိတ်ဆက်မှုတွေကို တားဆီးထားတဲ့အခါ[33]။
အင်တာနက်စာမျက်နှာ (website) အမည်များကို အိုင်ပီလိပ်စာ (IP) များအဖြစ် ပြောင်းလဲပေး သည့် လုပ်ငန်းစဉ် (DNS) ကိုခြယ်လှယ်ခြင်း	အင်တာနက်စာမျက်နှာ (website) အမည်များကို အိုင်ပီလိပ်စာ (IP) များအဖြစ် ပြောင်းလဲပေး သည့် လုပ်ငန်းစဉ် (DNS) ကိုဦးစီးလုပ်ကိုင်သူက က ပစ်မှတ်ထားတဲ့ အင်တာနက်စာမျက်နှာ အမည်တစ်ခုအတွက် အတုအယောင် အိုင်ပီလိပ်စာ (IP) တစ်ခုကို ပြန်ပေးတာ ဒါမှမဟုတ် ဘာအဖြေမှ ပြန်မပေးတာမျိုး ဖြစ်ပါတယ်[34]။
အင်တာနက်စာမျက်နှာ လိပ်စာအပြည့်အစုံ	ကြားခံဆက်သွယ်ပေးသူ (Proxy) က သင်သွားချင်တဲ့ အင်တာနက်စာမျက် နှာလိပ်စာပါ

[33] Electronic Frontiers Foundation, "How to: Understand and Circumvent Network Censorship," Surveillance Self-Defense, last modified February 01, 2024, https://ssd.eff.org/module/understanding-and-circumventing-network-censorship.

[34] Canadian Centre for Cybersecurity. "Domain Name System (DNS) tampering – ITSAP.40.021," cyber.gc.ca, published August 2022, https://www.cyber.gc.ca/en/guidance/domain-name-system-dns-tampering-itsap40021

(URL) ကိုစစ်ထုတ်ခြင်း	ခေါင်းစဉ် (Hyper Text Transfer Protocol (HTTP) Host header) ဒါမှမဟုတ် အင်တာနက်စာမျက်နှာ လိပ်စာအပြည့်အစုံ (URL) လမ်း ကြောင်း ကို ဖတ်ပြီး သတ်မှတ်ထားတဲ့ အင်တာနက် စာမျက်နှာတွေကို ပိတ်ဆို့ထားပေမဲ့ ကျန်တဲ့ အင်တာနက်စာမျက်နှာတွေကို တော့ ဝင်ရောက် ခွင့်ပေးတာကိုဆိုလိုပါသည်။
အချက်အလက်များကို အသေးစိတ် စစ်ဆေးခြင်း (DPI) နဲ့ အဓိက စကားလုံး စစ်ထုတ်ခြင်း	သတင်းအချက်အလက်အစုံလိုက်အပြီုလိုက်ထဲကအကြောင်းအရာတွေက ို သီးခြား စကားလုံးတွေ ၊ စကားစုတွေ (ဒါမှမဟုတ်) ထပ်ခါ ထပ်ခါဖြစ်နေတဲ့ ပုံစံတွေကို ရှာဖွေ စစ်ဆေးပါတယ်။ အချက်အလက်များကို အသေးစိတ် စစ်ဆေးခြင်း (DPI-Deep Packet Inspection) ကတော့ အင်တာနက် ပေါ်မှာသွားလာနေတဲ့သတင်းအချက်အလက်တွေရဲ့ ခေါင်းစဉ်သာမကဘဲ အထဲမှာပါတဲ့ သတင်းအချက်အလက်တွေ ကိုပါ ပိုမိုနက်ရှိုင်းစွာ စစ်ထုတ်တာ ကို ဆိုလိုပါသည် [35]။
အင်တာနက်တွင်သယ်ယူပို့ဆောင်ရေးဂိတ် သုံ စစ်ထုတ်ခြင်း	သတင်းအချက်အလက်သယ်ယူပို့ဆောင်မှု ကို သတင်းအချက် အလက် သယ်ယူပို့ဆောင်ရေး လုပ်ထုံးလုပ်နည်း နှင့် အင်တာနက်တွင် သယ်ယူ ပို့ဆောင်ရေး ဂိတ်နံပါတ် ကို အခြေခံ၍ ပိတ်ဆို့ သို့မဟုတ် ကန့်သတ် ထားသည် ကို ဆိုလိုပါသည် [36]။
အင်တာနက်မြန်နှုန်းလျှော့ချခြင်း	အင်တာနက်မြန်နှုန်း (Bandwidth) အသုံးမပြုနိုင်လောက်အောင် လျှော့ချ လိုက်ခြင်း ကို ဆိုလိုပါသည် [37]။
အင်တာနက် ဖြတ်တောက်ခြင်း	နိုင်ငံအဆင့် (သို့မဟုတ်) ဒေသအဆင့် အင်တာနက်ချိတ်ဆက်မှုတွေကို ရည်ရွယ်ချက်ရှိရှိ ပိတ်ချလိုက်တာဖြစ်ပါတယ်။ The Internet Society အဖွဲ့က က တစ်ကမ္ဘာလုံးဆိုင်ရာ အင်တာနက်ဖြတ်တောက်မှုတွေကို မှတ်တမ်းတင် ထားပါတယ်။ ၂၀၂၅ ခုနှစ်၊ ဧပြီလ အထိ နောက်ဆုံး ၁၂ လအတွင်း အင်တာနက် ဖြတ်တောက်မှုပေါင်း ၁၂၆ ခု ရှိခဲ့ပါတယ် [38]။

ကိုယ်ပိုင်ကွန်ရက်အတု (VPN)

ဆင်ဆာဖြတ်တောက်မှုအမျိုးမျိုးကို ကျော်လွှားဖို့အတွက် လိုအပ်တဲ့ ဒီကယ်ပေါက်/လွတ်ပေါက်အစရှိသည့် နည်းလမ်း တွေက ကွဲပြားပါတယ် ။ ဒီလိုလုပ်ဆောင်ဖို့အတွက် ကိုယ်ပိုင်ကွန်ရက်အတု (VPN) တွေဟာ အသုံးများတဲ့ ကိရိယာတစ်ခုဖြစ်ပြီး၊ ယခင်အခန်းရဲ့ ကိုယ်ရေးကိုယ်တာလုံခြုံမှု (Privacy)၊ လုံခြုံရေး (Securit) နဲ့ အမည်မဖော်လိုခြင်း (Anonymity) အမည်ဝှက်အပိုင်းမှာ ဆွေးနွေးပြီးဖြစ်ပါတယ်။ အနှစ်ချုပ်ပြောရရင် ကိုယ်ပိုင်ကွန်ရက်အတု (VPN) တွေဟာ သင့်ရဲ့အင်တာနက်အသွားအလာအတွက် လျှို့ဝှက်ကုဒ်သွင်းထားတဲ့

35 Christian Fuchs, "Societal and Ideological impacts of Deep Packet Inspection Internet Surveillance," *Information, Communication & Society 16*, no. 8, (2013): 1328-1359, https://doi.org/10.1080/1369118X.2013.770544.

36 Aliza Vigderman and Gabe Turner, "Internet censorship in 2025: The impact of Internet restrictions," *Security.org*, last modified August 22, 2024, https://www.security.org/vpn/internet-censorship/.

37 Samuel Woodhams, "The Rise of Internet Throttling: A Hidden Threat to Media Development," *Center for International Media Assistance*, May, 20, 2020, https://www.cima.ned.org/publication/the-rise-of-bandwidth-throttling-a-hidden-threat-to-media-development/

38 "Internet Shutdowns," The Internet Society, accessed June 15, 2025, https://pulse.internetsociety.org/en/shutdowns/

ဥမင်လိုဏ်ခေါင်းတွေလိုပါပဲ။ သင့်ရဲ့ချိတ်ဆက်မှုက ို တခြားနေရာမှာရှိတ ဲ့ ဆာဗာတွေကနေတစ်ဆင့် လမ်းကြောင်းလွဲပေးခြင်းဖြင့် သင့်ရဲ့ အိုင်ပီလိပ်စာ (IP) ကို ဖုံးကွယ်ပေးပါတယ်။ ဒါကြောင့် သင်ရဲ့ အင်တာနက် သုံးဆွဲမှုဆိုင် ရာလုပ်ဆောင်တောင်းဆိုချက်တွေက တခြားနိုင်ငံ (သို့မဟုတ်) ဒေသတစ်ခုကနေ လာတာလို့ ပေါ်လာစေပြီး ပထဝီဝင်ဆိုင်ရာ ကန့်သတ်ချက်တွေကို ကျော်လွှားနိုင်တာ ဖြစ်ပါတယ်။

ပုံမှန် ကိုယ်ပိုင်ကွန်ရက်အတ ွ (VPN) တစ်ခုက နိုင်ငံပြင်ပကနေ ထုတ်ပေးပြီး ပိတ်ဆို့ခံထားရတဲ့ သတင်းတွေ (သို့မဟုတ်) အချက်အလက်တွေကို ဖတ်ရှုနိုင်အောင် ကူညီပေးနိုင်ပါတယ်။ အင်တာနက်စာမျက်နှာတွေ၊ သတင်းဌာနတွေနဲ့ အင်တာနက်လူမှုကွန်ယက်မီဒီယာပလက်ဖောင်းတွေကို ပိတ်ဆို့ထားတဲ့ နိုင်ငံတွေမှာဆိုရင် တော့ ကိုယ်ပိုင်ကွန်ရက်အတ ွ (VPN) ဟာ တက်ကြွလှုပ်ရှားသူတွေကို ဒီကန့်သတ်ချက်တွေကို ကျော်လွှားပြီး ပွင့်လင်းမြင်သာတဲ့အင်တာနက်ကို လက်လှမ်းမှီစေပါတယ်။ သို့သော်လည်း ကိုယ်ပိုင်ကွန်ရက်အတ ွ (VPN) တွေ အားလုံးဟာ စွမ်းဆောင်ရည် မတူညီကြသလို၊ သူတို့ဟာ ဖုံးကွယ်ထားနိုင်တဲ့ မျက်နှာဖုံးတစ်ခုလည်း မဟုတ်ပါ ဘူး။ အချို့သော ဝန်ဆောင်မှုတွေက သင့်ရဲ့အချက်အလက်တွေကို မှတ်တမ်းတင်ထားနိုင်တယ်၊ သင့်ရဲ့အင်တာ နက်အမြန်နှုန်းကို လျှော့ချထိန်းချုပ်နိုင်တယ် (throttling) ဒါမှမဟုတ် သင့်ကို စောင့်ကြည့်မှုတွေ ပိုမိုခံရစေနိုင် ပါတယ်။ ဒါကြောင့် မှတ်တမ်းမသိမ်းဆည်းတဲ့ (no-log) ကိုယ်ပိုင်ကွန်ရက်အတ ွ (VPN) ဝန်ဆောင်မှုကို ရွေးချယ် ဖို့က အရေးကြီးပါတယ်။

ကောင်းမွန်တဲ့ ကိုယ်ပိုင်ကွန်ရက်အတ ွ (VPN) တစ်ခုကသင့်ကို လုပ်ငန်းလည်ပတ်မှု လုံခြုံရေး (OPSEC) မ ကောင်း ခြင်းကနေ မကာကွယ်ပေးနိုင်ပါဘူး။ ကိုယ်ပိုင်ကွန်ရက်အတ ွ (VPN) ချိတ်ဆက်ထားချိန်မှာ မည်သူ မည်ဝါဖြစ်ကြောင်း ဆုံးဖြတ်ပေးနိုင်တ ဲ့ ကိုယ်ပိုင်အချက်အလက်တွေန ဲ့ အီးမေး ဒါမှမဟုတ် ဖေ့စဘုတ် စာမျက်နှာ ကို ဝင်လိုက်တာနဲ့ သင့်ရဲ့ ကိုယ်ပိုင်ကွန်ရက်အတ ွ (VPN) သုံးစွဲမှုဟာ အဓိပ္ပာယ်မရှိတော့ပါဘူး။ လူအ များစု သတိမထားမိတဲ့ အဓိက အားနည်းချက်တစ်ခုဖြစ်တဲ့ ဘရောက်ဆာကနေတဆင့် အချက်အလက်တွေကို ခြေရာခံခြင်း (browser fingerprinting) ကနေလည်း ကိုယ်ပိုင်ကွန်ရက်အတ ွ (VPN) က သင့်ကို မကာကွယ် ပေးနိုင်ပါဘူး[39]။ သင့်ရဲ့ ကိုယ်ပိုင်အချက်အလက်တွေန ဲ့ ချိတ်ဆက်ထားတဲ့ ကိုယ်ပိုင် စက်ပေါ်မှာ ကိုယ်ပိုင် ကွန်ရက်အတ ွ (VPN) သုံးတာဟာလည်း အန္တရာယ် ရှိနိုင် ပါတယ်။

နိုင်ငံတွေရဲ့ ဆင်ဆာလုပ်တ ဲ့ နည်းလမ်းတွေဟာ တစ်နေ့ထက်တစ်နေ ့ ပိုပြီး ခေတ်မီတိုးတတ်လာပါတယ်။ အချက်အလက်များကို အသေးစိတ်စစ်ဆေးခြင်း (DPI) နဲ့ကွန်ယက်တွေကို စစ်ထုတ်ခြင်း (networking filtering) လိုမျိုး နည်းပညာတွေက အစိုးရတွေကို ကိုယ်ပိုင်ကွန်ရက်အတ ွ (VPN)ရဲ့ အင်တာနက် အချက်အလက်စီးဆင်းမှုတွေ တွေကို လုပ်ထုတ်လုပ်နည်း အဆင့် (protocol level) မှာတင် ဖော်ထုတ်နိုင်၊ ပိတ်ဆို့နိုင် ဒါမှမဟုတ် နှေးကွေးအောင် လုပ်နိုင်ပါတယ်။ သင့်ရဲ့ ကိုယ်ပိုင်ကွန်ရက်အတ ွ (VPN) က သင့်ကိုရေဒါ ကလွတ်စေတဲ့ နည်းလမ်း (stealth protocols) တွေကို မပံ့ပိုးဘူးဆိုရင် သင် ကိုယ်ပိုင်ကွန်ရက်အတ ွ (VPN)

[39] Kate Irwin, "Worried About Digital Privacy? VPNs and Tor Aren't Enough Anymore," *PC Mag*, November 4, 2024, https://www.pcmag.com/news/chelsea-manning-vpns-and-tor-arent-enough-for-digital-privacy.

သုံးစွဲနေတာကို အလွယ်တကူ သိရှိနိုင်ပါတယ်။ သင် ကိုယ်ပိုင်ကွန်ရက်အတွင်း (VPN) သုံးထားတဲ့ ဆိုတဲ့ အချက်အလက်တွေကို လျှို့ဝှက်ထားပေးတဲ့ (Obfuscation) နည်းပညာတွေသုံးထားရင်တောင် အစိုးရတွေက လွယ်ကူလျင်မြန်စွာ လိုက်လျောညီထွေ ပြုပြင်နိုင်ကြပါတယ်။ ဒါဟာ ကြောင်နဲ့ကြွက် ကစားပွဲတစ်ခုလိုပါပဲ။ ဒီလိုဖြစ်စဉ်မျိုးကို မြန်မာနိုင်ငံမှာ တွေ့မြင်နိုင်ပါတယ်[40]။

ကန့်သတ်ချက်တွေနဲ့ စိန်ခေါ်မှုတွေ ရှိနေပေမဲ့လည်း ကိုယ်ပိုင်ကွန်ရက်အတွင်း (VPN) ဟာ ဆင်ဆာဖြတ်တောက်တာတွေကို ရှောင်ရှားဖို့အတွက် အစွမ်းအထက်ဆုံး ကိရိယာတွေထဲက တစ်ခုအဖြစ် ရှိနေတုန်းပါပဲ။ ဒါပေမဲ့ ကိုယ်ပိုင်ကွန်ရက်အတွင်း (VPN) တစ်ခုတည်းနဲ့တော့ မလုံလောက်ပါဘူး။ စောင့်ကြည့်မှုနဲ့ ထိန်းချုပ်မှုတွေကို တကယ်ပဲ ရှောင်ကွင်းနိုင်ဖို့အတွက် ကိုယ်ပိုင်ကွန်ရက်အတွင်း (VPN) သုံးစွဲမှုကို ကောင်းမွန် တဲ့ လုပ်ငန်းလည်ပတ်မှု လုံခြုံရေး (OPSEC) နဲ့ ပေါင်းစပ်ပြီး အမြဲတမ်း လိုက်လျောညီထွေဖြစ်အောင် ပြောင်းလဲနေဖို့ လိုအပ်ပါတယ်။

ကြားခံဆက်သွယ်ပေးသူများ (Proxies)

ဆင်ဆာဖြတ်တောက်တဲ့ ကိစ္စရပ်တချို့မှာ ကြားခံဆက်သွယ်ပေးသူဆာဗာ (proxy server) သုံးရုံနဲ့ လုံလောက်နိုင်ပါ တယ်။ ကြားခံဆက်သွယ်ပေးသူဆာဗာ (Proxy server) ဆိုတာ သင့်ရဲ့ စက် နဲ့ အင်တာနက် ကြားက ကြားခံလူ (သို့) ကြားခံပစ္စည်းတစ်ခုအဖြစ် လုပ်ဆောင်ပါတယ်[41]။ ပိတ်ဆို့ခံထားရတဲ့ အင်တာနက်စာမျာ ကို တိုက်ရိုက်ချိတ်ဆက် မယ့်အစား သင့်ရဲ့ တောင်းဆိုချက်ကို ကြားခံဆက်သွယ်ပေးသူ (proxy) ကနေတစ်ဆင့် လမ်းကြောင်းပြောင်းသွားမှာဖြစ်ပြီး၊ ကြားခံဆက်သွယ်ပေးသူ (proxy) က သင့်ကိုယ်စား တောင်းဆိုချက်ကို ထပ်ဆင့်ပို့ပေးမှာ ဖြစ်ပါတယ်။ အိုင်ပီလိပ်စာ (IP) ကိုပိတ်ဆို့ခြင်း (IP blocking) နဲ့ အင်တာနက်စာမျက်နှာလိပ်စာအပြည့်အစုံကို စစ်ထုတ်ခြင်း (URL filtering) တွေကို ကျော်လွှားဖို့ ကြိုးစားနေတယ်ဆိုရင် proxy တွေက ကောင်းကောင်း အလုပ်လုပ်နိုင်ပါတယ်။

ကြားခံဆက်သွယ်ပေးသူ (Proxy) အမျိုးအစားတွေ အများကြီးရှိပါတယ်။ ဥပမာအားဖြင့် **HTTP** ကြားခံဆက်သွယ်ပေးသူ တွေက HTTP/S လုပ်ထုံလုပ်နည်းကနေလာတဲ့ လာတဲ့ အင်တာနက်သတင်းအချက်အလက် စီးဆင်းမှု ကိုပဲ ကိုင်တွယ်ပါတယ်။ ဒါနဲ့ပြောင်းပြန်ဖြစ်တဲ့ SOCKS ကြားခံဆက်သွယ်ပေးသူ တွေကတော့ အင်တာနက် ဘရောက်ဆာ (web browsing) အပြင် တခြား အင်တာနက်သတင်းအချက်အလက် စီးဆင်းမှု တွေကိုလည်း ကိုင်တွယ်ပေးနိုင်ပါတယ်[42]။ ကြားခံဆက်သွယ်ပေးသူ (Proxy) တွေက ပြီးပြည့်စုံတဲ့ နည်းလမ်းတစ်ခုလို

---

40 Allegra Mendelson, “Cat and mouse: Myanmar netizens find cracks in draconian VPN ban,” *Frontier Myanmar*, August 6, 2024, https://www.frontiermyanmar.net/en/cat-and-mouse-myanmar-netizens-find-cracks-in-draconian-vpn-ban/

41 Michael Buckbee, “What is a proxy server and how does it work?”, *Varonis* (blog), June 24, 2022, https://www.varonis.com/blog/what-is-a-proxy-server

42 Vejune Tamuliunaite, “SOCKS vs HTTP Proxy: What Is the Difference?,” *Oxylabs*, May 30, 2025, https://oxylabs.io/blog/socks-vs-http-proxy.

ထင်ရပေမဲ့ အန္တရာယ်ကင်းတယ်လို့တော့ မဆိုနိုင်ပါဘူး။ အခကြေးငွေပေးစရာမလိုတဲ့ ကြားခံဆက်သွယ်ပေးသူဆာဗာ (proxy server) အများစုဟာ အစိုးရတွေ ဒါမှမဟုတ် ရန်လိုတဲ့ ပြင်ပအဖွဲ့အစည်းတွေက လုပ်ထားတဲ့ ပျားရည်သုတ်လိမ်းထားတဲ့ ထောင်ချောက်တွေ ဖြစ်နိုင်ပါတယ်။ ကြားခံဆက်သွယ်ပေးသူ (Proxy) တွေက သင့်ရဲ့ အင်တာနက်သတင်း အချက်အလက် စီးဆင်းမှု ကို လျှို့ဝှက်ကုဒ်အဖြစ်ပြောင်းလဲမှု (encrypt) မလုပ်ပေးတဲ့အတွက် သင့်ရဲ့ လုပ်ဆောင် တောင်းဆိုမှုတွေကို အလွယ်တကူ စောင့်ကြည့်ပြီး ပိတ်ဆို့လို့ရနေတုန်းပါပဲ။ V2Ray လိုမျိုး ဒီကိစ္စအတွက် ကူညီပေးနိုင်တဲ့ ကြားခံဆက်သွယ်ပေးတဲ့ ကိရိယာ တချို့ရှိပေမဲ့ ဒါတွေကလည်း အမြဲတမ်းစိတ်ချ ရတယ်လို့ မဆိုနိုင်ပါဘူး[43]။

နည်းပညာပိုင်းဆိုင်ရာ ရှုပ်ထွေးတဲ့ တပ်ဆင်တည်ဆောက်မှု တွေနဲ့ လုပ်ထားရုံနဲ့ အလိုအလျောက် လုံခြုံစိတ်ချရပြီလို့ မမှတ်ယူ သင့်ပါဘူး။ တခြား ကိရိယာတွေလိုပဲ လုံခြုံရေးဆိုတာ ဘယ်လို တပ်ဆင်တည်ဆောက် ထားလဲ၊ ဘယ်လောက်အထိ သတိထားသုံးစွဲလဲဆိုတာပေါ်မှာ လုံးလုံးလျားလျား မူတည်ပါတယ်။ ကြားခံဆက်သွယ်ပေးသူ တွေနဲ့ ပတ်သက်ပြီးတော့ သူတို့ရဲ့ ကန့်သတ်ချက်တွေကို နားလည်ထားဖို့ လိုအပ်ပါတယ်။ အထူးသဖြင့် သူတို့ဟာ ကိုယ်ရေးကိုယ်တာလုံခြုံရေး (privacy) နဲ့ လုံခြုံရေး (security) အတွက် ရည်ရွယ်ပြီး တည်ဆောက်ထားတာ မဟုတ်ဘူးဆိုတာကို သိထားရပါမယ်။

အင်တာနက်စာမျက်နှာ အမည်များကို အိုင်ပီလိပ်စာ (IP) *များအဖြစ် ပြောင်းလဲပေး သည့် လုပ်ငန်းစဉ် (DNS)*

ဆင်ဆာလုပ်တဲ့ နည်းလမ်းတွေထဲက အင်တာနက်စာမျက်နှာ အမည်များကို အိုင်ပီလိပ်စာ (IP) များအဖြစ် ပြောင်းလဲပေး သည့် လုပ်ငန်းစဉ် (DNS) ကိုခြယ်လှယ်ခြင်း (DNS tampering) ဒါမှမဟုတ် အဆိပ်ခပ်ခြင်း (poisoning) ကိစ္စတွေဟာ အချက်အလက်များကို အသေးစိတ်စစ်ဆေးခြင်း (DPI) ထက်ကျော်လွှားဖို့ ပိုပြီး ရိုးရှင်းပါတယ်။ တစ်ခါတလေမှာ အင်တာနက်စာမျက်နှာ အမည်များကို အိုင်ပီလိပ်စာ (IP) များအဖြစ် ပြောင်း လဲပေး သည့် လုပ်ငန်းစဉ် (DNS) လုပ်ဆောင်သည့်ဆာဗာ (DNS resolver) တစ်ခုကို ပြောင်းလဲ လိုက်ရုံနဲ့ အဆင်ပြေနိုင်ပါတယ်[44]။ ဥပမာ - Google ရဲ့ အများသိတဲ့ အင်တာနက်စာမျက်နှာ အမည်များကို အိုင်ပီလိပ် စာ (IP) များအဖြစ် ပြောင်းလဲပေး သည့် လုပ်ငန်းစဉ် (DNS) (8.8.8.8, 8.8.4.4), Cloudflare DNS (1.1.1.1) ဒါမှမဟုတ် Quad9 (9.9.9.9) တို့ကို ပြောင်းသုံးခြင်းဖြင့် မှန်ကန်တဲ့ အင်တာနက်စာမျက်နှာ အမည်များကို အိုင်ပီလိပ်စာ (IP) များအဖြစ် ပြောင်းလဲပေး သည့် လုပ်ငန်းစဉ် (DNS) ရလဒ်တွေကို ရရှိပြီး ပြည်တွင်းက ပြုပြင်ပြောင်းလဲပြီးပိတ်ဆို့ထားမှုတွေကို ကျော်လွှားနိုင်ပါတယ်။ ဒါပေမဲ့ တချို့နိုင်ငံတွေမှာတော့ ဒီ အမျ အင်တာနက်စာမျက်နှာ အမည်များကို အိုင်ပီလိပ်စာ (IP) များအဖြစ် ပြောင်းလဲပေး သည့် လုပ်ငန်းစဉ် (DNS) လုပ်ဆောင်သ

[43] Linus Lorentzen, "What is V2Ray, and how does it work?," *Doprax* (blog), June 21, 2023, https://www.doprax.com/privacy/what-is-v2ray-and-how-can-you-use-it/.

[44] Jacinta Wothaya, "What is Censorship and What Tools Can SJOs Use to Bypass Restricted Content?," *Tatua Digital Resilience Centre*, September 2, 2024, https://tatua.digital/services/what-is-censorship-and-what-tools-can-sjos-use-to-bypass-restricted-content/

ည့်ဆာဗာ (DNS servers) တွေကိုတောင် ပိတ်ဆို့ထားတာ ဒါမှမဟုတ် သူတို့ရဲ့ အင်တာနက်သတင်း အချက်အလက် စီးဆင်းမှု တွေကို ကြားဖြတ်ပြီး ပြောင်းလဲပစ်တာတွေ လုပ်ပါတယ်။ ဒီနေရာမှာ လျှို့ဝှက်ကုဒ် အဖြစ်ပြောင်းလဲထားတဲ့ အင်တာနက်စာမျက်နှာ အမည်များကို အိုင်ပီလိပ်စာ (IP) များအဖြစ် ပြောင်းလဲပေး သည့် လုပ်ငန်းစဉ် (DNS) လုပ်ထုံးလုပ်နည်း (encrypted DNS protocols) တွေက အရေးပါလာပါတယ်။ DNS over HTTPS (DoH) နဲ့ DNS over TLS (DoT) တို့ဟာ အင်တာနက်စာမျက်နှာ အမည်များကို အိုင်ပီလိပ်စာ (IP) များအဖြစ် ပြောင်းလဲပေး သည့် လုပ်ငန်းစဉ် (DNS)ကမေးခွန်း တွေကိုယ်တိုင်ကို လျှို့ဝှက်ကုဒ်အဖြစ်ပြောင်းလဲ ပေးပါတယ်။ ဒီနည်းပညာနှစ်ခုက သင်တောင်းဆိုတဲ့ ဆာဗာ တွေဆီကနေ ရလဒ်တွေကို ရရှိတာကို အာမခံပေး နိုင်ပေမဲ့၊ အကယ်၍ အစိုးရက အင်တာနက်စာမျက်နှာ အမည်များကို အိုင်ပီလိပ်စာ (IP) များအဖြစ် ပြောင်းလဲ ပေး သည့် လုပ်ငန်းစဉ် (DNS) လုပ်ဆောင်သည့်ဆာဗာ (DNS servers) တွေကို ရလဒ်တွေ ပြောင်းလဲခိုင်းရင် တော့ သင့်ကို မကာကွယ်နိုင်ပါဘူး။ အင်တာနက်စာမျက်နှာ အမည်များကို အိုင်ပီလိပ်စာ (IP) များအဖြစ် ပြောင်းလဲပေး သည့် လုပ်ငန်းစဉ် (DNS)လုပ်ဆောင်သည့်ဆာဗာ (Resolvers) တွေကိုယ်တိုင်က ထိခိုက်နေပြီဆို ရင် DoH နဲ့ DoT တို့က သိပ်အကူအညီမဖြစ်နိုင်တော့ပါဘူး။ ဒီလိုအခြေအနေမျိုးမှာတော့ ဒိုမိန်းအမည်စနစ် လုံခြုံရေး တိုးချဲ့မှုများ (DNSSEC) က အကူအညီပေးနိုင်ပါတယ်။ ဒိုမိန်းအမည်စနစ် လုံခြုံရေး တိုးချဲ့မှုများ (DNSSEC) ဆိုတာ သင်လက်ခံရရှိတဲ့ အင်တာနက်စာမျက်နှာ အမည်များကို အိုင်ပီလိပ်စာ (IP) များအဖြစ် ပြောင်းလဲပေး သည့် လုပ်ငန်းစဉ် (DNS) ရလဒ်တွေဟာ တရားဝင်ရင်းမြစ် (authoritative source) ကနေ လာ တာဟုတ်မဟုတ် စစ်ဆေးအတည်ပြုနိုင်တဲ့ သတ်မှတ်ချက်တွေ ဖြစ်ပါတယ်။

သတင်းအချက်အလက်တွေကို လမ်းလှမ်းမှီဖို့အတွက် ဆင်ဆာဖြတ်တောက်မှုကို ကျော်လွှားတာနဲ့၊ သတင်း အချက် အလက်တွေ ထုတ်ပြန်ဖို့အတွက် ဆင်ဆာဖြတ်တောက်မှုကို ကျော်လွှားတာဟာ မတူညီဘူးဆိုတာကို ခွဲခြားသိမြင်ဖို့ လိုအပ်ပါတယ်။ တိုရွန်တိုတက္ကသိုလ်က Citizen Lab ဟာ ဒီနှစ်ခုကြားက ကွာခြားချက်ကို ရှင်းပြ ထားတဲ့ ပြည့်စုံတဲ့ လမ်းညွှန်တစ်ခုကို ရေးသားခဲ့ပါတယ်[45]။ သတင်းအချက်အလက်ကို လမ်းလှမ်းမှီရယူဖို့ ကြိုးစားခြင်းဟာ အင်တာနက်မှာ သတင်းအချက်အလက်တွေ ထုတ်ပြန်တာထက် အနုနည်းဖြင့် သွယ်ဝိုက်အာခံ ဖိဆန်ခြင်း (Passive defiance) ပုံစံမျိုး ပိုဆန်ပါတယ်။ သတင်းအချက်အလက်တွေ ထုတ်ပြန်တာကတော့ ခြိမ်းခြောက်မှုပုံစံ (threat model) ကို လုံးဝပြောင်းပြန်လှန် လိုက်ပါတယ်။ သတင်းအချက်အလက်တွေထုတ် ပြန်တာကို ဖျက်လိုဖျက်ဆီးလုပ်ရပ် (subversive) အဖြစ် ရှုမြင်ပါတယ်။ ဘာလို့လဲဆိုတော့ ဒါက တခြားသူတွေ ကို ပိတ်ပင်ထားတဲ့ အယူအဆတွေကို ရယူနိုင်စေတာရယ်၊ အာဏာရှင်အစိုးရတိုင်း အဆိုးဆုံးကြောက်တဲ့ အရာ ဖြစ်တဲ့ အတိုက်အခံအင်အားစုတွေကို စုစည်းနိုင်စေတာကြောင့်ပါ။ ဒါကြောင့်မို့ ဒီနေရာမှာပဲ အပြင်းထန်ဆုံး ဆင်ဆာလုပ်တာတွေနဲ့ စောင့်ကြည့်မှုတွေ စုစည်းအာရုံစိုက်နေတာ ဖြစ်ပါတယ်။

တော(Tor) ကွန်ယက် နဲ့တောင်မှ ထုတ်ပြန်ဖို့အတွက် သတိထားပြီး သီသန့်စဉ်းစားစီစဉ်တာမျိုး လုပ်ဖို့ လိုအပ်ပါ တယ်။ တော (Tor) ကွန်ယက် ကနေတစ်ဆင့် အခြား လျှို့ဝှက်ထားပေးတဲ့ (obfuscation) ဒါမှမဟုတ် ကြားခံ

[45] The Citizen Lab, *Everyone's guide to by-passing Internet censorship* (The Citizen Lab, 2007), https://citizenlab.ca/guides/everyones-guide-english.pdf.

တွေ (bridges) တွေမပါဘဲ အရေးကြီးတဲ့ ဖိုင်တွေကို အင်တာနက်ကွန်ယက်ပေါ်တင်တာမျိုး (upload) လုပ်တာဟာ အာရုံစိုက်မှုကို ခံရနိုင်ပါသေးတယ်။ ဒီလိုအခြေအနေမျိုးမှာ ဆင်ဆာကို ကျော်လွှားဖို့ လိုအပ်တဲ့ နည်းလမ်းတွေဟာ ရှုပ်ထွေးတဲ့ လုပ်ငန်းလည်ပတ်မှု လုံခြုံရေး (OPSEC) တစ်ခု လိုအပ်ပါတယ်။

ဇယား ၃- ဆင်ဆာဖြတ်တောက်မှုတွေကို ကျော်လွှားရာမှာ အကူအညီဖြစ်နိုင်တဲ့ နည်းလမ်းများ (ပြည့်ပြည့်စုံစုံ မဟုတ်နိုင်ပါ)။

ကိရိယာ	**လုပ်ဆောက်ချက်**	**ပလက်ဖောင်း**	**F-droid[46] ပလက်ဖောင်းတွင် ရှိ/မရှိ**	**အင်တာနက် လိပ်စာ**	**မှတ်ချက်**
OONI Probe	အင်တာနက်ဆင်ဆာ ဖြတ်တောက် မှုကို တိုင်းတာပေးခြင်း	Linux, Android, iOS, Win, macOS, Linux	ရှိ	https://ooni.org/install/all/	
Mullvad ကိုယ်ပိုင်ကွန်ယက်အတု (VPN)	အင်တာနက် လှုပ်ရှားမှုများ ကို မှတ် တမ်းတင်မထားသော ကိုယ်ပိုင် ကွန်ယက်အတု (VPN) ဝန်ဆောင်မှု	Linux, Android, iOS, Win, macOS	ရှိ	https://mullvad.net/en/pricing	ကြည့်ရန်- Mullvad ၏ ဆင်တာ ကိုကျော်ဖြတ်သော အဆင့်မြင့်နည်းပညာ[47]
Proton ကိုယ်ပိုင်ကွန်ယက်အတု (VPN)	အင်တာနက် လှုပ်ရှားမှုများ ကို မှတ်တမ်းတင်မထားသော ကိုယ်ပိုင်ကွန်ယက်အတု (VPN) ဝန်ဆောင်မှု	Linux, Android, iOS, Win, macOS	ရှိ	https://protonvpn.com/	ကြည့်ရန်- Proton ရဲ့ ရေဒါက လွတ်စေတဲ့ နည်းလမ်း[48]
V2Ray	အင်တာနက် လုံခြုံရေး ကို တိုးမြှင့်စေပြီး၊ ဆင် ဆာဖြတ် တောက်မှုကို ကျော်လွှားဖို့ ရည်ရွယ် ထုတ်လုပ်ထားတဲ့ အဆင်မြှင့် ကြားခံဆက်သွယ် ပေးသော ကိရိယာ	Linux, Win, macOS	မရှိ	https://www.v2ray.com/en/	
Psiphon	အင်တာနက်ပေါ်က အကြောင်းအရာတွေကို ဆင်ဆာမဲ့ ဝင်ရောက် နိုင်ဖို့ ကိုယ်ပိုင်ကွန်ယက်	Android, iOS, Win, macOS	မရှိ	https://psiphon.ca/en/psiphon-	

[46] "What is F-droid?," F-droid, accessed June 15, 2025, https://f-droid.org/

[47] "Introducing Shadowsocks Obfuscation for WireGuard," Mullvad, published October 25, 2024 https://mullvad.net/en/blog/introducing-shadowsocks-obfuscation-for-wireguard

[48] "Defeat censorship with Stealth, our new VPN protocol", ProtonVPN, October 6, 2022, https://protonvpn.com/blog/stealth-vpn-protocol

	အတု (VPN), လုံခြုံစိတ်ချရေသာ အကာ (SSH) နဲ့ HTTP ကြားခံ ဆက်သွယ်နည်းပညာတွေကို အသုံးပြုပါတယ်။			guide.html#psiphonguide_section1	
Riseup ကိုယ်ပိုင် ကွန်ယက်အတု (VPN)	အင်တာနက် လှုပ်ရှားမှုများ ကို မှတ် တမ်းတင်မထားသော ကိုယ်ပိုင် ကွန်ယက်အတု (VPN) ဝန်ဆောင်မှု	Linux, macOS, Win, Android	ရှိ	https://riseup.net/en/vpn	
Tor ဘရောက်ဆာ	Tor ကွန်ယက်ကို အသုံးပြုပြီး လျှို့ဝှက်စွာ အင်တာနက် အသုံးပြု နိုင်ဖို့ ရည်ရွယ်ဖန်တီး ထားတဲ့ အလွှာ တွေအများကြီးနဲ့ ကွန်ယက် ဘရောက်ဆာ တစ်မျိုး ဖြစ်ပါတယ်။	Linux, Android, Win, macOS	မကြာမီ[49]	https://www.torproject.org/download/tor/	
Onion ဘရောက်ဆာ	iOS စနစ်အတွက် Tor ဘရောက်ဆာ	iOS	ရှိ	https://apps.apple.com/us/app/onion-browser/id519296448	ကြည့်ရန်- Onion ဘရောက်ဆာ သုံးသပ်ချက်[50]
Orbot	Tor မှတစ်ဆင့် မည်သည့် အပလီကေးရှင်းများကို အသုံးပြုမည်ဆိုတာ သင့်ကိုသီးခြားရွေးချယ်ခွင့် ပြုနိုင်	Android, iOS, macOS	ရှိ	https://orbot.app/en/	
Lantern	ဆိုဒ်တစ်ခု ပိတ်ဆို့ခံထားရခြင်း ရှိမရှိကို ရှာဖွေပြီးနောက် ၎င်း၏ဆာဗာမှတစ်ဆင့် ထိုဆိုဒ်ကို ဝင်ရောက်စေပါသည်။	Linux, Android, Win, macOS, iOS		https://lantern.io/	
Tails	TAILS သို့မဟုတ် 'The Amnesiac Incognito Live System' သည် ကိုယ်ရေးကိုယ်တာလုံခြုံမှု (Privacy) ကို အဓိကထားပြီး ဖန်တီးထားသည့် Debian-အခြေခံ ကွန်ပျူတာစက်လည်ပတ်ရေးစနစ်) (OS) တစ်ခု	Linux, Win, macOS		https://tails.net/	

[49] "Is Tor Browser available on F-droid?," Tor, accessed June 15, 2025, https://support.torproject.org/tormobile/tormobile-7/.

[50] "Onion Browser Review: Tor on iOS," Privacy Guides, accessed June 15, 2025, https://www.privacyguides.org/articles/2024/09/18/onion-browser-review/.

	ဖြစ်သည်။				
I2P	အပြည့်အဝ လျှို့ဝှက်ကုဒ်အဖြစ် ပြောင်းလဲမှု (encrypt)လုပ်ထားပြီး၊ မည်သူမည်ဝါဖြစ်ကြောင်းဖော် ထုတ်မရအောင် ပြုလုပ်ပေးထားတဲ့ တိုက်ရိုက်ချိတ်ဆက်ပြီး အလယ် ဗဟို ဆာဗာမရှိ ဆက်သွယ်မှုဝ ခွင့်ပြုခြင်း (Peer-to-peer) ဆက် သွယ်မှုတွေကို ခွင့်ပြုပေးတဲ့ ကိုယ် ပိုင်ကွန်ယက် အလွှာတစ်ခု ဖြစ်ပါ တယ်။	Linux, Android, macOS, Win,	ရှိ	https://geti2p.net/en/	
RethinkDNS + Firewall	အက်ပလီကေးရှင်းရဲ့ လုပ်ဆောင်ချက်တွေကို စောင့်ကြည့်ပြီး အင်တာနက် ဆင်ဆာဖြတ်တောက်မှုတွေကို ကျော်လွှားပေးပါတယ်။	Android	ရှိ	https://rethinkdns.com/app	
Censorship.no	ပါဝင်သူများအချင်းချင်း အင်တာနက်စာမျက်နှာများကို တိုက်ရိုက်ချိတ်ဆက်ပြီး အလယ် ဗဟို ဆာဗာ မရှိ ဆက်သွယ်မှုဝ ခွင့်ပြုခြင်း (peer-to-peer) နည်းပညာဖြင့် ဖြန့်ဝေပေးသည့် အင်တာနက် ဘရောက်ဆာ တစ်ခု။	Linux, Android, Win	ရှိ	https://censorship.no/	

စောင့်ကြည့်ခြင်း

တက်ကြွလှုပ်ရှားသူတွေ ရင်ဆိုင်ရတဲ့ နောက်ထပ်အဖြစ်များတဲ့ ခြိမ်းခြောက်မှုတစ်ခုကတော့ စောင့်ကြည့်ခံရခြင်း (surveillance) ပဲဖြစ်ပြီး၊ ဒါဟာ ဆင်ဆာဖြတ်တောက်တာနဲ့ အတူယှဉ်တွဲ ဆက်စပ်နေပါတယ်။ အစိုးရတစ်ရပ်အနေနဲ့ လူပုဂ္ဂိုလ်တစ်ဦးတစ်ယောက်ချင်းစီအလိုက်၊ ကိုယ်ပိုင်အချက်အလက်တွေ၊ အဖွဲ့အစည်းတွေ (Bodies) နဲ့ အတွေးအခေါ်တွေကို ဆင်ဆာလုပ်ဖို့အတွက် သူတို့က လူတွေကို စောင့်ကြည့်ဖို့ မဖြစ်မနေ လိုအပ်ပါတယ်။ စောင့်ကြည့်တာဟာ ဘယ်သူကလုပ်သလဲဆိုတာပေါ်မူတည်ပြီး ပုံစံအမျိုးမျိုး ရှိပါတယ်။ နည်းပညာကုမ္ပဏီ အကြီးကြီးတွေစီက စောင့်ကြည့်တာကို ခံနေရသလား။ နည်းပညာ ကုမ္ပဏီ အကြီးကြီးတွေစီက စောင့်ကြည့်တာကို ခံနေရကို Zuboff က အရင်းရှင်စနစ်ရဲ့ စောင့်ကြည့်တာခံနေရခြင်း (Surveillance capitalism)လို့ ခေါ်ပါတယ်[51]။ သာမန်ပြည်သူတွေ ကနေတစ်ဆင့် နေ့စဉ်လှုပ်ရှားမှုတွေကိုအပြန်အလှန်စောင့်ကြည့်တာကို ခံနေ

[51] Shoshana Zuboff, *The Age of Surveillance Capitalism* (PublicAffairs, 2019).

ရပါသလား။ ဒီလို စောင့်ကြည့်တာကို Mann ကတော့ ပြင်သစ်စကားလုံး အောက် (sous) ကို အစားထိုးပြီး 'Sousveillance' လို့ ခေါ်ဝေါ်ခဲ့ပါတယ်[52]။ စောင့်ကြည့်တာဟာ ဘယ်တော့မှ ကြားနေဘက်မလိုက်ဘဲ ရှိနေတာမျိုးမဟုတ်ပါဘူး။ ဒါဟာ မတူညီတဲ့ အာဏာအဆင့်အတန်းတွေကြားက ဆက်ဆံရေးတစ်ခု အမြဲဖြစ်နေပါတယ်။ စောင့်ကြည့်ရုံသာမကဘဲ၊ ဘယ်သူက စောင့်ကြည့်ရမယ့်သူစာရင်းထဲ ပါရမလဲဆိုတာကို အင်တာနက်လုပ်ထုံးလုပ်နည်းတွေနဲ့ ဆုံးဖြတ်တဲ့ ညဏ်ရည်တု (AI) အခြေခံ စောင့်ကြည့်ရေးစနစ်တွေ တိုးတက်လာတာနဲ့အမျှ၊ ကျွန်တော်တို့ဟာ Sisyphus လိုပဲ Tartarus တောင်ကုန်းပေါ်ကို ကျောက်တုံးကြီးကို အဆုံးမရှိ တွန်းတင်နေရတဲ့အခြေအနေမျိုးနဲ့ ရင်ဆိုင်နေရပါတယ်။

NSA ရဲ့ ရှိသမျှအရာအားလုံးစုဆောင်းခြင်း (collect it all) နည်းလမ်းကနေ ကျွန်တော်တို့ကို ပြောပြနေတဲ့ အရာတစ်ခုရှိ တယ်ဆိုရင် အဲဒါက စောင့်ကြည့်မှုဟာ အဓိကအားဖြင့် ထိန်းချုပ်မှုအတွက် ဖြစ်တယ်ဆိုတာပါပဲ။ စောင့်ကြည့်ခံနေရတယ်ဆိုတဲ့ သဘောတရားတစ်ခုတည်းနဲ့တင် လူတွေရဲ့ အတွေးအခေါ်တွေ မတွေးတာ မပေါ်ပေါက်ခင်မှာတင် လိုက်နာဖို့နဲ့ နှုတ်ဆိတ်နေဖို့ ဖိအားတွေ ဖြစ်ပေါ်စေပါတယ်။

စောင့်ကြည့်ခံရခြင်းဟာ လူရယ်လို့ဖြစ်စေတဲ့ အခြေခံအကျဆုံးဖြစ်တဲ့ လွတ်လပ်စွာ တွေးတောခွင့် ကို ချိုးဖောက်တာ ဖြစ်ပါတယ်။

အချိန်ကြာလာတာနဲ့အမျှ စောင့်ကြည့်မှုဟာ လူမှုအသိုင်းအဝိုင်းမှာကြီးစိုးနေတဲ့ အမြင်တွေကို ပြန်တွန်းလှန်ဖို့ စိတ်အားထက်သန်မှု နည်းပါးတဲ့ မျိုးဆက်သစ်တွေကို မွေးထုတ်ပေးပါတယ်[53]။ Monahan ပြောခဲ့သလိုပါပဲ၊ "ကျင့်ဝတ်နဲ့ညီတဲ့ စောင့်ကြည့်မှုဆိုတာ စောင့်ကြည့်တာမရှိခြင်းပါပဲ"[54]။ စောင့်ကြည့်မှု (surveillance) အလေ့အကျင့်ဟာ တက်ကြွလှုပ်ရှားသူတွေနဲ့ အတိုက်အခံတွေကို အကြမ်းဖက်သမား၊ အဖျက်သမား၊ ကွန်မြူနစ် တံဆိပ်တပ်ခြင်းတွေ (red-tagging) နဲ့ ပုဂ္ဂိုလ်ရေးဆိုင်ရာ အချက်အလက်တွေကို ခိုးယူပြီး အင်တာနက်ပေါ်မှာ ဖော်ထုတ်(doxxing) အပါအဝင် အခြားသော ဒစ်ဂျစ်တယ် ဖိနှိပ်မှုပုံစံတွေကိုလည်း အားပေးပါတယ်။ တက်ကြွလှုပ်ရှားသူတွေနဲ့ အတိုက်အခံတွေကို အကြမ်းဖက်သမား၊ အဖျက်သမား၊ ကွန်မြူနစ် တံဆိပ်တပ်ခြင်းတွေ (red-tagging) ဆိုတာကို အရင်အပိုင်းမှာ အကျဉ်းချုပ် ဖော်ပြခဲ့ပြီးပါပြီ။ ဒါဟာ စစ်အေးတိုက်ပွဲကာလ (Cold War) ရဲ့ အတွေးအခေါ်ထဲမှာ အမြစ်တွယ်နေတဲ့ ၊ အထူးသဖြင့် အမေရိကန်နိုင်ငံရဲ့ နိုင်ငံခြားရေးမူဝါဒကနေ ကမ္ဘာအနှံ့ ပျံ့နှံ့သွားတဲ့ ကွန်မြူနစ် တစ္ဆေ ခြောက်ခံရခြင်းထဲမှာ အမြစ်တွယ်နေတဲ့ နှိပ်စက်ညှဉ်းပန်းမှုတစ်မျိုးဖြစ်တယ် ဆိုတာကို ကျွန်တော်တို့ သိထားပြီးပါပြီ။ ဖိလစ်ပိုင်နိုင်ငံမှာ တက်ကြွလှုပ်ရှားသူတွေနဲ့ အတိုက်အခံတွေကို အကြမ်းဖက်သမား၊ အဖျက်သမား၊ ကွန်မြူနစ် တံဆိပ်တပ်ခြင်းတွေ (red-tagging) ကို

---

52 Steve Mann, "Sousveillance: Secrecy, not privacy, may be the true cause of terrorism," 2002, accessed June 10, 2025, http://www.wearcam.org/sousveillance.htm.

53 Christopher Pines, *Ideology and false consciousness: Marx and his historical progenitors* (SUNY Press, 1993).

54 Torin Monahan, "On the impossibility of ethical surveillance," in *The Handbook of Communication Ethics*, eds. Amit Pinchevski, Patrice M Buzzanell and Jason Hannan (Routledge, 2022), 320-331. http://dx.doi.org/10.2139/ssrn.4129499

McCarthyism ရဲ့ ပုံစံအတိုင်း အတိအကျယူသုံးခဲ့ပါတယ်။ ဒါဟာ မြေယာပိုင်ဆိုင်ခွင့်၊ အလုပ်သမား အခွင့်အရေး၊ ဌာနေတိုင်းရင်းသားတွေရဲ့ အချုပ်အချာအာဏာ စတာတွေနဲ့ ပတ်သက်တဲ့ လူပ်ရှားမှုတွေကို လက်နက်ကိုင်တော်လှန်ရေး ဒါမှမဟုတ် အကြမ်းဖက်မှုနဲ့ ဆက်စပ်ပြီး စွပ်စွဲတာ ဖြစ်ပါတယ်။ ဖိလစ်ပိုင်ရဲ့ နိုင်ငံတော် ဥပဒေရေးရာ မဟာဗျူဟာတွေမှာ ဒီလိုလုပ်ဆောင်နေတာကို တွေ့ခဲ့ရပြီး၊ အင်တာနပ် ဝါဒဖြန့်ချိမှုတွေ နဲ့ လူအများအပြားအုပ်စုလိုက် စောင့်ကြည့်တာမျိုးတွေကို (mass surveillance) အရှိန်မြှင့်ပေးခဲ့ပါတယ်[55]။ မကြာသေးမီက ဗီဒီယို၊ အသံနှင့်ဓာတ်ပုံများစွာကိုသုံးပြီး ဗီဒီယိုအတု ဖန်းတီးသောနည်းပညာ (deepfakes) နဲ့ ညစ်ထ်ရည်တုနဲ့ သုံးပြီး ဘာသာစကားတွေနားလည်ရေးသာနိုင်သောနည်းပညာ (large language models) တွေကို အသုံးပြုမှု မြင့်တက်လာတာက တက်ကြွလှုပ်ရှားသူတွေနဲ့ အတိုက်အခံတွေကို အကြမ်းဖက်သမား၊ အဖျက်သမား၊ ကွန်မြူနစ် တံဆိပ်တပ်ခြင်းတွေ (red-tagging) လုပ်ငန်းစဉ်ကို ပိုပြီး မြန်ဆန်စေပါတယ်။ ဒါကို ၂၀၂၅ ခုနှစ် ကြားဖြတ်ရွေးကောက်ပွဲများကာလမှာ ထင်ရှားစွာ တွေ့မြင်ခဲ့ရပါတယ်။ ကွန်ပျူတာပညာရှင်များ သမဂ္ဂ (Computer Professionals Union) ရဲ့တွေ့ရှိချက်အရ ရွေးကောက်ပွဲမတိုင်ခင်မှာ တက်ကြွလှုပ်ရှားသူတွေနဲ့ အဖွဲ့အစည်းတွေကို အကြမ်းဖက်သမား၊ အဖျက်သမား၊ ကွန်မြူနစ် တံဆိပ်တပ်ခြင်းတွေ (red-tagging) လုပ်တဲ့ ဗီဒီယို၊ အသံနှင့်ဓာတ်ပုံ များစွာကိုသုံးပြီး ဗီဒီယိုအတု ဖန်းတီးသောနည်းပညာ (deepfakes) နဲ့ ညစ်ထ်ရည်တု (AI) ကထုတ် စာသားတွေကို ပျံ့နှံ့စေတဲ့ ဖေ့စဘုတ် စာမျက်နှာ အနည်းဆုံး ၁၄ ခုကို တွေ့ရှိခဲ့ရပါတယ်[56]။ တစ်စုံတစ်ဦး ကို ရှာတွေ့ပြီးတာနဲ့ အုပ်စုလိုက်တညီတညွတ်တည်း အကောင့်တုများစွာသုံးပြီး ဝါဒဖြန့်သော လုပ်ရပ် (troll farms) တွေကို အသုံးပြုပြီး အဲဒီပုဂ္ဂိုလ်ရဲ့ ပုဂ္ဂိုလ်ရေးဆိုင်ရာ အချက်အလက်တွေကို ခိုးယူပြီး အင်တာနက်ပေါ်မှာ ဖော်ထုတ် (doxxing) ပါတော့တယ်။ ဒီလုပ်ငန်းစဉ်ဟာ အကြမ်းဖက်သမား၊ အဖျက်သမား၊ ကွန်မြူနစ် တံဆိပ်တပ် (red tagged**)** ခံရသူကို အန္တရာယ်ရှိတဲ့သူအဖြစ် အများပြည်သူသိအောင် ပြောဆိုပြီး အမြဲတမ်း ခြေရာခံနိုင်တဲ့ အချက်အလက်တွေအဖြစ် ပြောင်းလဲပစ်လိုက်ပါတယ်။ ဒီအရာအားလုံးဟာ တရားဥပဒေလုပ်ထုံးလုပ်နည်းများ (due process)၊ သက်သေအထောက်အထားများနှင့် အများအား ဖြင့် အရင်းအမြစ်တွေမလိုဘဲနဲ့ ဖြစ်ပေါ်လာခြင်း ဖြစ်သည်။

ဆင်ဆာဖြတ်တောက်တာတွေကို ကျော်လွှားတုန်းကလိုပဲ စောင့်ကြည့်ခံရခြင်းကို ရှောင်ရှားဖို့အတွက် သင့်ရဲ့ ခြိမ်းခြောက်ခံရမှုအဆင့် (threat level) ကို ကောင်းကောင်းနားလည်ထားဖို့ လိုအပ်ပါတယ်။ **ခြိမ်းခြောက်ခံရမှု ပုံစံ (threat modelling) မေးခွန်းတွေရဲ့** အဖြေတွေက သင့်ရဲ့ ကိရိယာတွေ၊ နည်းဗျူဟာတွေနဲ့ ဆက်သွယ်ရေးနည်းလမ်းတွေနဲ့ ပတ်သက်တဲ့ ဆုံးဖြတ်ချက်တိုင်းကို လမ်းညွှန်ပေးပါလိမ့်မယ်။ အကယ်၍ သင်ဟာ စီးပွားရေးလုပ်ငန်းကြီးတွေရဲ့ ခြေရာခံခြင်းကို ရှောင်ချင်တဲ့ အန္တရာယ်အလားအလာနည်းတဲ့ (low-risk) သူတစ်ယောက်ဖြစ်တယ်ဆိုရင် ဘရောက်ဆာကိုပိုလုံခြုံအောင်သုံးခြင်း (browser hardening) ၊ အင်တာနက်

---

55 Amnesty International, *Philippines: "I turned my fear into courage": Red-tagging and state violence against young human rights defenders in the Philippines* (Amnesty International, 2024), https://www.amnesty.org/en/documents/asa35/8574/2024/en/.

56 Computer Professionals' Union, "#Eleksyon2025Watch — RED-HANDED: REPORT ON SOCIAL MEDIA RED-TAGGING DURING THE ELECTION PERIOD" Facebook, May 18, 2025, https://www.facebook.com/story.php?story_fbid=1130518759115014&id=100064707008190&_rdr.

လှုပ်ရှားမှုစောင့်ကြည့်ခြင်းကို တားဆီး ပေးသောအရာ (tracker blockers) နဲ့ ကောင်းမွန်တဲ့စကားဝှက် တွေ ထားရှိရုံနဲ့ လုံလောက်နိုင်ပါတယ်။ ဒါပေမဲ့ သင်ဟာ ဝေဖန်ပြောဆိုမှုကြောင့် သင့်ဘဝ ဒါမှမဟုတ် သင့်မိသားစုရဲ့ ဘဝ တွေကို အန္တရာယ်ရှိစေနိုင်တဲ့ နိုင်ငံ တစ်ခုက တက်ကြွလှုပ်ရှားသူတစ်ဦးဆိုရင်တော့ သင်ဟာ ကြီးမားတဲ့ စောင့်ကြည့်နိုင်စွမ်းရှိတဲ့ နိုင်ငံတော်အဆင့်ရှိ သူနဲ့ရင်ဆိုင်နေရတာ ဖြစ်ပါတယ်။ ဒီအခြေအနေနှစ်ခုအတွက် မ တူညီတဲ့ လုပ်ငန်းလည်ပတ်မှုလုံခြုံရေး (OPSEC) နှစ်မျိုးလိုအပ်ပါတယ်။

စက်ပစ္စည်းများအားစောင့်ကြည့်ခြင်း

ယေဘူယျအားဖြင့် လူတစ်ဦးဟာ တစ်နှစ်ကို ပျမ်းမျှအားဖြင့် ၈၈ ရက်လောက် ဖုန်းသုံးကြပါတယ်[57]။ ဒါကြောင့် ကျွန်တော် တို့ရဲ့ နေ့စဉ်ဘဝတွေမှာ ဒီနည်းပညာအပေါ် အလွန်အမင်း မှီခိုလာကြတယ်ဆိုတာကို သံသယဖြစ်စရာ မလိုပါဘူး။ ကျွန်တော်တို့ရဲ့ ဖုန်းတွေထဲမှာ အတွင်းရေးကျတဲ့ ကိုယ်ရေးအချက်အလက်တွေ၊ သူငယ်ချင်း၊ မိသားစုနဲ့ လုပ်ဖော်ကိုင်ဖက်တွေရဲ့ ဖုန်းနံပါတ်စာရင်းတွေ ပါဝင်ပါတယ်။ ဒါကြောင့် သင့်ဖုန်းကို ထိုးဖောက်ဝင် ရောက်ခံရရင် သင့်ဘဝလည်း ထိခိုက်နိုင်တယ် ဆိုတာ အံ့သြစရာ မဟုတ်ပါဘူး။ တက်ကြွလှုပ်ရှားသူတွေ အတွက်တော့ ဒါဟာ အဆပေါင်းများစွာ အန္တရာယ် ပိုများပါတယ်။ အသုံးပြုသူအတွက် အဆင်ပြေစေဖို့ ရောင်းချထားတဲ့ စမတ်ဖုန်းရဲ့ စွမ်းဆောင်ချက်တွေဟာ ကျွန်တော်တို့ရဲ့ လှုပ်ရှားမှု တွေနဲ့ တည်နေရာတွေကို ခြေရာခံပြီး မှတ်တမ်းတင်နိုင်အောင် ရည်ရွယ်ပြီး ဒီဇိုင်းထုတ်ထားခြင်းဖြစ်ပါသည်။ နည်းပညာ ကုမ္ပဏီကြီးများ ၊ ဆက်သွယ်ရေး ကုမ္ပဏီ များနှင့် အစိုးရများသည် ဒီအချက်အလက်များအားလုံး မည်မျှတန်ဖိုးရှိသည်ကို သိရှိ ကြပါတယ်။ ဒါကြောင့် သင့်မိုဘိုင်းလ်စက် ပစ္စည်းများ၏ ထိခိုက်နိုင်ခြေနဲ့ ထိစပ်မှုတွေကို မည်သို့ကန့်သတ်ရ မည်ကို အပြည့်အဝနားလည်ထားရန် အရေးကြီး ပါသည်။

အလွယ်ကူဆုံး ချဉ်းကပ်နည်းတစ်ခုကတော့ မူလတပ်ဆင်ထားသည့်အတိုင်း မပြောင်းလဲတဲ့ အခင်းအကျင်း (stock) Android နဲ့ iOS တွေကို လုံးဝ စွန့်လွှတ်လိုက်ဖို့ပါပဲ။ GrapheneOS လိုမျိုး ပိုမိုလုံခြုံမှုရှိတဲ့လုပ်ငန်း လည်ပတ်မှုစနစ် (hardened operating systems**)** တွေက သင့်ဖုန်းရဲ့ အချက်အလက်ပေါက်ကြားနိုင်မှုကို ပို ပြီးထိရောက်စွာ ထိန်းချုပ်နိုင်ပါတယ်။ ကံမကောင်းစွာနဲ့ပဲ GrapheneOS ကို Pixel (Google ကုမ္ပဏီထုတ်) ဖုန်း တွေအတွက်ပဲ ရရှိနိုင်ပြီး Google ရဲ့ စောင့်ကြည့်မှုကို Google ကထုတ်တဲ့ ဖုန်းနဲ့ ပြန်တိုက်ထုတ်ရတာဟာ သရော်စာလိုမျိုး ဖြစ်နေပါတယ်။ GrapheneOS အဖွဲ့ ရဲ့ ပြောကြားချက်အရ လက်ရှိအချိန်မှာ (Google ကုမ္ပဏီထုတ်) Pixel ဖုန်းတွေဟာ သူတို့ရဲ့ တင်းကျပ်တဲ့ ဟာ့ဒ်ဝဲနဲ့ လုံခြုံရေးစံနှုန်းတွေကို ပြည့်မီတဲ့ တစ်ခုတည်း သော စက်ပစ္စည်းတွေပဲ ဖြစ်ပါတယ်[58]။

---

57 Serena Smith, “We spend 88 days a year on our phones,” *Dazed*, April 25, 2025, https://www.dazeddigital.com/life-culture/article/66669/1/we-spend-88-days-a-year-on-our-phones-addiction-mental-health-loneliness.

58 “Frequently Asked Questions,” Grapheneos.org, accessed June 24, 2025, https://grapheneos.org/faq#future-devices

ဒါပေမဲ့ အခုချက်ချင်း ဖုန်း ဒါမှမဟုတ် လုပ်ငန်းလည်ပတ်မှုစနစ် (operating system) ပြောင်းလဲဖို့ မဖြစ်နိုင်သေးဘူး ဆိုရင်တောင် အန္တရာယ်ကို လျှော့ချနိုင်တဲ့ နည်းလမ်းတွေ ရှိပါသေးတယ်။ iOS သုံးစွဲသူများအနေဖြင့် မလိုအပ်သော ဒေတာမျှဝေမှုနှင့် တိုက်ခိုက်ခံနိုင်ခြေရှိသော အခြေအနေများကို လျှော့ချရန်အတွက် တည်နေရာညွှန်ပြခြင်းဝန်ဆောင်မှု၊ ဘလူးတု ဝန်ဆောင်မှု၊ iOS ရဲ့အချက်အလက်မျှဝေခြင်း ဝန်ဆောင်မှု (airdrop)၊ အပလီကေးရှင်းများကိုအလိုအလျောက် ပြန်ဖွင့်ပေးတဲ့ ဝန်ဆောင်မှု (background app ကဲ့သို့သော လုပ်ဆောင်မှုများကို ပိတ်ထားနိုင်ပါသည်။ မိမိအတွက်သီးသန်းလုပ်ထားသောကြော်ညာ များကို ပိတ်ထားခြင်း၊ သတင်းအချက်အလက်တွေကို အလိုအလျောက် စုဆောင်း၊ မျှဝေ၊ ခွဲခြမ်းစိပ်ဖြာမှုလုပ်ငန်းစဉ် (telemetry) ကိုပိတ်ထားခြင်းနှင့် ဆီရီ (Siri) ကိုဖုန်းလော့ချထားစဉ် ဝင်ရောက်ခွင့်ကို ကန့်သတ်ခြင်းတို့သည်လည်း အထောက်အကူဖြစ်စေနိုင်ပါသည်[59]။ Android သုံးစွဲသူများအနေဖြင့်မူ ပိုမိုလုံခြုံအောင် ပြုလုပ်နိုင်ပါသည်။ သင့်ဖုန်းတွင် Google ဝန်ဆောင်မှုများ အသုံးပြုနေပါက သင့်စက်ပစ္စည်းသည် အလိုအလျောက် ကြော်ငြာ အမှတ်အသား (ID) တစ်ခုကို ထုတ်လုပ်နေကြောင်း သိထားသင့်သည်။ ကြော်ငြာခြေရာခံခြင်းကို လျှော့ချရန် ၎င်းကို ပိတ်နိုင်သည် သို့မဟုတ် ဖျက်ပစ်နိုင်သည်။ အခြားသိမှတ်ဖွယ်အကြံပြုချက်တစ်ခုမှာ အသုံးပြုသူ ပရိုဖိုင်များသို့မဟုတ် ကိုယ်ပိုင်နေရာများ သတ်မှတ်ထားခြင်း ဖြစ်သည်။ ယင်းတို့သည် အပလီကေးရှင်းများနှင့် အချက်အလက်များကို သီးခြားခွဲထားရန် ကူညီပေးနိုင်သဖြင့် သင့်ဖုန်းကို အခြားသူများနှင့် မျှဝေသုံးစွဲခြင်း သို့မဟုတ် ကိုယ်ရေးကိုယ်တာနှင့် အလုပ်ကိစ္စနှစ်မျိုးစလုံးအတွက် အသုံးပြုခြင်းတို့တွင် အထောက်အကူဖြစ်စေသည် [60]။

ဆန္ဒပြပွဲတက်ရောက်တဲ့အခါ မိုဘိုင်းဖုန်း လုံခြုံရေး လမ်းညွှန်

လူအများနဲ့စုဝေးစည်းရုံးပြီး တည်ဆောက်ရာမှာ ကျွန်တော်တို့ရဲ့ ဖုန်းတွေဟာ မရှိမဖြစ်တဲ့ ကိရိယာတစ်ခု ဖြစ်လာတယ်ဆိုတာကို ကျွန်တော်တို့ သိပြီးသားပါ။ ဒါပေမဲ့ ဆန္ဒပြပွဲတွေနဲ့ ပတ်သက်လာတဲ့အခါမှာတော့ ဖုန်းဟာ အားသာချက်တစ်ခု ဖြစ်မလာဘဲ အားနည်းချက်တစ်ခုလို ဖြစ်လာပါတယ်။ The Markup အဖွဲ့က ၂၀၂၀ ပြည့်နှစ်မှာ ပြည့်စုံတဲ့ လမ်းညွှန်တစ်ခုကို ရေးသားခဲ့ပြီး ၂၀၂၄ မှာ ပြန်လည်ပြင်ဆင်ခဲ့ပါတယ်[61]။ သူတို့ရေးသားခဲ့တာတွေဟာ အထူးသဖြင့် ဆန့်ကျင်တော်လှန်ရေးလုပ်ငန်းတွေ လုပ်ဆောင်နေသူတွေအတွက် အရေးကြီးပြီး လက်ရှိအချိန်နဲ့ ကိုက်ညီနေဆဲပါပဲ။ ဒီမှာဖော်ပြထားတဲ့ အကြံပြုချက်တွေနဲ့ နည်းလမ်းတွေဟာ The Markup အဖွဲ့ရဲ့ လမ်းညွှန်ချက်ထဲကနေ ယူထားတာဖြစ်ပေမဲ့ မြောက်အမေရိကဘက်က မဟုတ်တဲ့ လူတွေအတွက် ပိုပြီး သင့်လျော်မယ့် အပြောင်းအလဲတွေနဲ့ ရှင်းလင်းချက်တချို့ကို ထည့်သွင်းထားပါတယ်။

---

59 Privacy Guides, “iOS Overview,” accessed June 24, 2025, https://www.privacyguides.org/en/os/ios-overview/

60 Privacy Guides, “Android Overview,” accessed June 24, 2025, https://www.privacyguides.org/en/os/android-overview/#safetynet-and-play-integrity-api

61 Dan Phiffer, Tomas Apodaca, Miles Hilton and Maddy Varner, “How Do I Prepare My Phone for a Protest? (Updated 2024),” *The Markup*, May 4, 2024, https://themarkup.org/the-breakdown/2024/05/04/how-do-i-prepare-my-phone-for-a-protest-updated-2024

သင့်ရဲ့ အသုံးများတဲ့အဓိကပင်မဖုန်း (Primary Phone) ကို အိမ်မှာထားခဲ့တာဟာ ဒစ်ဂျစ်တယ် စောင့်ကြည့်ခံရခြင်းကို ရှောင်ရှားနိုင်ဖို့ အထိရောက်ဆုံး နည်းလမ်းတစ်ခု ဖြစ်နိုင်ပါတယ်။ ဒါကတော့ ဖိနှိပ်မှုနဲ့ စောင့်ကြည့်မှုတွေ အားကောင်းတဲ့ ဒေသတွေမှာ နေထိုင်သူတွေအတွက် ပိုပြီးမှန်ပါတယ်။ အကယ်၍ သင်ဟာ ဆက်သွယ်ချိတ်ဆက်ဖို့ တစ်ခုတည်းသော အကြောင်းပြချက်နဲ့ ဖုန်းယူဆောင်သွားမယ်ဆိုရင်တော့ ရိုးရှင်းတဲ့ လုပ်ဆောင်ချက်တွေပဲ ပါဝင်တဲ့ ဒုတိယဖုန်းတစ်လုံး (secondary phone) ကို သုံးစွဲနိုင်ပါတယ်။ သင့်ကိုမည်သူမည်ဝါဖြစ်ကြောင်း ဖော်ထုတ်ပေးနိုင်တဲ့ ကိုယ်ပိုင်အချက်အလက်တွေနဲ့ မချိတ်ဆက်ထားတဲ့ မတူညီတဲ့ ဖုန်းကတ် (SIM card) တစ်ခုကိုလည်း သုံးစွဲဖို့ စဉ်းစားသင့် ပါတယ်။

အကယ်၍ သင်က အသုံးများတဲ့အဓိကပင်မဖုန်းကို ယူသွားဖို့ ဆုံးဖြတ်ထားရင် သင်ဟာ သင်ရဲ့ဖုန်းကိုပဲ သယ်သွားတာ မဟုတ်ဘူးဆိုတာကို နားလည်ထားရပါမယ်။ အဲဒီဖုန်းဟာ ရုတ်တရက်ချက်ချင်းဆိုသလို သင့်ကိုရော၊ တခြားသူတွေကိုပါ အန္တရာယ်ဖြစ်စေနိုင်တဲ့ သက်သေခံပစ္စည်းတစ်ခုနဲ့ ခြေရာခံကိရိယာတစ်ခု ဖြစ်သွားနိုင်ပါတယ်။ အပြင်မထွက်ခင်မှာ သင့်ဖုန်းထဲက ကိုယ်ရေးကိုယ်တာ ဒါမှမဟုတ် သင်မည်သူမည်ဝါ လဲဆိုတာ သိနိုင်တဲ့ ကိုယ်ရေးကိုယ်တာ အချက်အလက်မှန်သမျှကို ဖယ်ရှားပစ်ဖို့ အချိန်ယူပါ။ ဖုန်းပိတ်ထားစဉ် ဖုန်းမျက်နှာပြင် (lock screen) မှာရှိတဲ့ ကိုယ်ပိုင်ဓာတ်ပုံတွေ၊ မိသားစုဓာတ်ပုံတွေ ဒါမှမဟုတ် တတ်ကြွလှုပ်ရှားမှုနဲ့ပတ်သတ်ပြီး ပို့စတာတွေကို ဖယ်ရှားလိုက်ပါ။ သင်ဘယ်သူလဲ၊ ဘာအတွက်ရပ်တည်လှုပ်ရှားနေလဲဆိုတာကို မဖော်ပြနိုင်တဲ့ ရိုးရိုးနောက်ခံပုံတစ်ခုကို ရွေးချယ်ပါ။

ဖုန်းပိတ်ထားစဉ် ဖုန်းမျက်နှာပြင်မှာ ပေါ်လာတဲ့ အသိပေးချက်တွေကိုလည်း (lock-screen notifications) တွေကိုလည်းသေချာပေါက် ပိတ်ထားသင့်ပါတယ်။ ဘာလို့လဲဆိုတော့ ဖုန်းကို သော့ဖွင့် (unlock) မလုပ် ဘဲနဲ့တောင်မှ ဒီ သတိပေးချက် တွေကနေ အရေးကြီးတဲ့ စကားပြောဆိုမှုတွေ ဒါမှမဟုတ် အသေးစိတ်အချက် အလက် တွေကို ပေါက်ကြားစေနိုင်ပါတယ်။ဒါ့အပြင် လက်ဗွေရာ ဒါမှမဟုတ် သင့်မျက်နှာမှတ်သားထားမှု လိုမျိုး ဇီဝဆိုင်ရာ အချက်အလက်တွေ သုံးပြီး သော့ ဖွင့်တဲ့ (biometric unlock) စနစ်တွေကိုပါ ဖယ်ရှားပစ်သင့်ပါတယ်။ အဲဒီအစား တစ်ယောက်ယောက်က သင့်ကို အတင်းအကျပ် ဖိအားပေးပြီး မဖွင့်ခိုင်းနိုင်တဲ့ ခိုင်မာတဲ့ နံပတ် (PIN) ဒါမှမဟုတ် လျှို့ဝှက်စာစု (passphrase) ကိုပဲ သုံးပါ။ သင့်လုပ်ဖော်ကိုင်ဖက်တွေနဲ့ ဆက်သွယ်တဲ့အခါ အဆုံးမှအဆုံး အချက်အလက်တွေကို လျှို့ဝှက်ကုဒ် အဖြစ်ပြောင်းလဲ ခြင်း စနစ်သုံးတဲ့ အပလီကေးရှင်း (end-to-end encrypted app) တွေကို သုံးပြီး ပို့ထားတဲ့ အချက် အလက်တွေ အလိုအလျောက် ပျောက်ကွယ်သွားတဲ့ (disappearing messages) ကို သေချာဖွင့်ထားဖို့ လိုပါတယ်။ စစ်ကနယ် အပလီကေးရှင်းသုံးစဉ် လုံခြုံရေးတိုးမြှင့်ပေးတဲ့ (Signal fork) အပလီကေးရှင်းတစ်ခုဖြစ်တဲ့ Molly ကလည်း သင့်သတင်းအချက်တွေကို သိမ်းဆည်းထားချိန်မှာပါ လျှို့ဝှက်ကုဒ် အဖြစ်ပြောင်းလဲ (encrypted) လုပ်ပေးပါတယ်။

အပေါ်ကဏ္ဍမှာ ဆွေးနွေးခဲ့တဲ့အတိုင်း လုပ်ငန်းလည်ပတ်မှုလုံခြုံရေး (OPSEC-Operational Security) ဆိုတာ အရေးကြီးပါတယ်။ ဘယ် စုဖွဲ့ ဆွေးနွေးနိုင်တဲ့ ကွန်ယက် (group chat) ထဲကိုပဲ သတင်းအချက်အလက်တွေ မ

ပို့ခင်မှာ မည်သူမည်ဝါ ဆိုတာဆုံးဖြတ်ပေးနိုင်တဲ့ မျက်နှာပါတာတွေကို ဖျက်တာ ဒါမှမဟုတ် ဝါးသွားအောင် လုပ်ထားတာ၊ ဓာတ်ပုံတွေမှာ အရေးကြီးတဲ့ အချက်အလက် (EXIF data) မပါတာကို သေချာပါစေ။ အနည်းဆုံး အနေနဲ့ ဘလူးတု (Bluetooth), ဝိုင်ဖိုင် (Wifi), အသံကိုအသုံးပြုပြီး စေခိုင်းသောစနစ် (Voice assistants) နဲ့ iOS ရဲ့အချက်အလက်မျှဝေခြင်း ဝန်ဆောင်မှု (Airdrop) လိုမျိုး အနီးအနားမှာရှိတဲ့တခြားစက်ပစ္စည်းတွေနဲ့ အချက်အလက်တွေမျှဝေတဲ့ ကိရိယာတွေကို ပိတ်ထားဖို့ အရေးကြီးပါတယ်။ အကောင်းဆုံးကတော့ ဖုန်းကို လေယာဉ်ပျံ ပုံစံ (airplane mode) ထဲကို ထည့်ထားတာပါပဲ။ IMSI ဖမ်းသူများ (IMSI catchers) လိုမျိုး စောင့်ကြည့်ရေးကိရိယာတွေဟာလည်း အနောက်နိုင်ငံတွေမှာတင်မကဘဲ တစ်ကမ္ဘာလုံးမှာ ပိုပြီး အဖြစ်များလာပါတယ်[62]။ ဒီ အယောင်ဆောင်ကလာပ်စည်း တာဝါတိုင် (fake cell tower) တွေဟာ သင့်ရဲ့ခန့်မှန်းခြေတည်နေရာကို သိနိုင်၊ ဖုန်းနံပါတ်ပိုင်ရှင်ကို ရှာနိုင်သလို၊ ခေါ်ဆိုမှုတွေနဲ့ သတင်းအချက်အလက် ဆက်သွယ်ပေးပို့မှုတွေကို အနှောင့်အယှက်ပေးနိုင်ပြီး စောင့်ကြည့်ဖို့ ပိုလွယ်ကူတဲ့ 2G အင်တာနက်ကွန်ယက်ကို သင့် 4G ကွန်ရက်က ကနေ ပြောင်းလဲဖို့ အတင်းအကျပ်ပြောင်းခိုင်းနိုင်ပါတယ်။

IMSI ဖမ်းသူများ ဆိုတာဘာလဲ

IMSI ဖမ်းသူများ ဆိုတာ နိုင်ငံတကာမိုဘိုင်းအသုံးပြုသူကိုယ်ရေးကိုယ်တာအချက်များက ို့ ဖမ်းယူသူ (International Mobile Subscriber Identity catcher) ရဲ့ အတိုကောက် ဖြစ်ပြီး သူ့ရဲ့ ရည်ရွယ်ချက်က မိုဘိုင်းဖုန်း အချက်ပြမှုတွေကို ကြားဖြတ်ယူဖို့ ဖြစ်ပါတယ်။ IMSI ဖမ်းသူတွေဟာ တရားဝင် ဆယ်လူလာ တာဝါတိုင်တွေလို ဟန်ဆောင်ပြီး ဖုန်းတွေကို ချိတ်ဆက်မိအောင် လှည့်ဖြားပါတယ်။ ချိတ်ဆက်မိတာနဲ့ IMSI ဖမ်းသူတွေဟာ သင့်ရဲ့ ဆင်းကတ် (SIM) ကနေ နိုင်ငံတကာမိုဘိုင်းအသုံးပြုသူကိုယ်ရေးကိုယ်တာအချက် (IMSI) နံပါတ်၊ ဖုန်းနံပါတ်နဲ့ တစ်ခါတလေ အချက်အလက် စာသား (SMS) (သို့) ဖုန်းခေါ်ဆိုမှုဆိုင်ရာ အရေးကြီးတဲ့ အချက်အလက် တွေလိုမျိုး မည်သူမည်ဝါဆိုတာ ကို သတ်မှတ် နိုင်တဲ့ အချက်အလက်တွေကို ဖမ်းယူနိုင်ပါတယ်။

နယ်စပ်ဖြတ်ကျော်ရာတွင် မိုဘိုင်းဖုန်း လုံခြုံရေး လမ်းညွှန်

နယ်စပ်ဖြတ်ကျော်ချိန်မှာ လက်ထဲမှာ မိုဘိုင်းဖုန်းပါလာရင် ထူးခြားတဲ့ အန္တရာယ်တွေ ရှိလာနိုင်ပါတယ်၊ အထူးသဖြင့် တတ်ကြွလှုပ်ရှားသူတွေအတွက် အာဏာရှင်အစိုးရတွေ ဒါမှမဟုတ် စိစစ်မှုတင်းကျပ်တဲ့ နယ်စပ်ထိန်းချုပ်မှုတွေ ရှိတဲ့ ဒေသတွေကို ဒါမှမဟုတ် ဒီ ဒေသတွေကနေ ခရီးသွားတဲ့အခါမျိုးမှာ ပိုအရေးကြီးပါတယ်။ ပထမဆုံးအနေနဲ့ နားလည်ပြီး အရှိတရားကို လက်ခံထားရမှာကတော့ နိုင်ငံများစွာမှာရှိတဲ့ လူဝင်မှုကြီးကြပ်ရေး အရာရှိတွေနဲ့ နယ်စပ်ရဲတွေမှာ သင့်ရဲ့ မိုဘိုင်းဖုန်းအပါအဝင် ကိုယ်ပိုင်စက်ပစ္စည်းတွေကို ရှာဖွေဖို့ လိုသလိုဆွဲဆ

[62] Araceli Ramirez, "IMSI catchers in Paraguay: the invisible surveillance threatening your right to protest," *TEDIC*, May 19, 2025, https://www.tedic.org/en/imsi-catchers-in-paraguay-the-invisible-surveillance-threatening-your-right-to-protest/

နှိုင်တဲ့ တစ်ခါတလေဆိုရင် အကန့်အသတ်မရှိသလောက် အခွင့်အာဏာတွေ ရှိတယ်ဆိုတဲ့ အချက်ပါပဲ။ နယ်စပ်မှာ ငြင်းခုန်တာဟာ သင့်ရဲ့ရုပ်ပိုင်းဆိုင်ရာဘေးကင်းလုံခြုံမှုကို သိသိသာသာ အန္တရာယ်ဖြစ်စေနိုင်ပြီး ချက်ချင်းပြန်ပို့တာ၊ ဖမ်းဆီးတာ ဒါမှမဟုတ် အချိန်ကြာမြင့်စွာ ထိန်းသိမ်းခံရတာမျိုးတွေထိ ဖြစ်နိုင်ပါတယ်။ သင့်ရဲ့ လူမျိုး၊ နိုင်ငံရေးအမြင် ဒါမှမဟုတ် နိုင်ငံသားအဆင့်အတန်းကြောင့် သင့်အတွက် အန္တရာယ်ပိုများနေတာ ဆိုရင်တော့ ဒါဟာ ပိုပြီးရှုပ်ထွေးနိုင်တဲ့အပြင် ချက်ချင်း ညင်းဆန်ခံရပြီးနောက် ရုပ်ပိုင်းဆိုင်ရာ အန္တရာယ် ဒါမှမဟုတ် ဖမ်းဆီးထိန်းသိမ်းခံရတာမျိုး ချက်ချင်းဖြစ်ပေါ်လာနိုင်ပါတယ်။ Electronic Frontiers Foundation (EFF)အဖွဲ့က အမေရိကန်နယ်စပ်ကို ဖြတ်ကျော်တဲ့အခါ သင့်ရဲ့အချက်အလက်တွေ ကို ဘယ်လိုကာကွယ်မလဲဆိုတဲ့ အစီရင်ခံစာတစ်ခု ရေးသားခဲ့ပါတယ်[63]။ အကြံပြုချက်အများစုက တခြားနေရာတွေ မှာလည်း အသုံးပြုနိုင်ပေမယ့် တချို့အကြံပြုချက်တွေကတော့ အထူးသဖြင့် နယ်စပ်ဖြတ်ကျော်နေရတဲ့ အခြေအနေမှာ ရှိတဲ့ လူနည်းစုတွေ နဲ့ နိုင်ငံသားအဆင့်အတန်းအမျိုးမျိုးရှိတဲ့သူတွေအတွက် အပိုအချက်အလက်တွေ လိုအပ်နိုင်ပါတယ်။

The Guardian သတင်းဌာန နဲ့ အင်တာဗျူးတစ်ခုမှာ EFF အဖွဲ့က Sophia Cope က သင့်ဖုန်းကို ဘယ်တော့မှ မဖျက်ပစ်ဖို့ အကြံပြုခဲ့ပါတယ်[64]။ ဘာလို့လဲဆိုတော့ အဲဒါက သံသယ များပိုမို တိုးပွားစေနိုင်လို့ပါပဲ။ အဲဒီအစား နယ်စပ်မရောက် ခင်မှာ သင်မပြချင်တဲ့/မမြင်စေချင်တဲ့ အချက်အလက်တွေဖြစ်တဲ့ သရောက်ဆာ မှတ်တမ်း၊ ဆက်သွယ်ပြောဆို ထားသော သတင်းအချက်အလက်မှတ်တမ်းများ၊ အီးမေး၊ ဓာတ်ပုံနဲ့ ဗီဒီယိုတွေကို ဖျက်လိုက်ပါ။ အထဲမှာ ဘာအကြောင်းအရာမှမရှိတဲ့ ဖုန်းအလွတ်တစ်လုံးကို မပြသင့်ပါဘူး။ သင့်ဖုန်းကို လော့ခ်ဖွင့်ခိုင်းတဲ့အခါမှာ သင့်ရဲ့ လျှို့ဝှက်နံပတ် (pin code) ကို ကိုယ်တိုင်ရိုက်ထည့်တာက အကောင်းဆုံးပါပဲ။ လျှို့ဝှက်နံပတ် (pin code) ကို မျှဝေလိုက်တာက ရေရှည်အကျိုးဆက်တွေ ရှိနိုင်ပါတယ်။ အထူးသဖြင့် တချို့နိုင်ငံတွေမှာ အရာရှိတွေဟာ သင့်ရဲ့ လျှို့ဝှက်နံပတ် (passcode) ကို မှတ်သားထားတာ ဒါမှမဟုတ် ဝင်ခွင့်ရလိုက်ပြီဆိုရင် ဖုန်းတစ်ခုလုံးမှာရှိတဲ့ သတင်းအချက်အလက်တွေအားလုံးကို ထုတ်ယူထိန်းသိမ်း (backup) တောင် ထားနိုင်ပါတယ်။ ဒီနေရာမှာ ကိရိယာထဲက အချက်အလက်အားလုံးကို လျှို့ဝှက်ကုဒ်အဖြစ်ပြောင်းလဲခြင်း နည်းစနစ် (disk encryption) ရဲ့ အရေးပါပုံ ပေါ်လာပါတယ်။ ကိရိယာထဲက အချက်အလက်အားလုံးကို လျှို့ဝှက်ကုဒ်အဖြစ်ပြောင်းလဲခြင်း နည်းစနစ် (disk encryption) က သင့်ရဲ့ လျှို့ဝှက်နံပတ် (passcode) နဲ့ သော့မဖွင့်ထားသရွေ့ အထဲကအချက်အလက် တွေဟာ လျှို့ဝှက်ကုဒ်ထားထားတဲ့အတွက် နားမလည်နိုင်တဲ့အနေအထား အတိုင်းပဲ ရှိနေမယ်ဆိုတာ သေချာစေပါတယ်။ တစ်စုံတစ်ယောက်က အချက်အလက် သိုလှောင်ရာပစ္စည်း (storage chip) ကနေ တိုက်ရိုက်ထုတ်ယူဖို့ ကြိုးစားရင်တောင်မှပဲ နားမလည်နိုင်တဲ့အနေအထား အတိုင်းပဲ ရှိနေမှာ ဖြစ်ပါတယ်။ ခေတ်မီဖုန်းအများစုက ဒီလုပ်ဆောင်ချက်ကို အလိုအလျောက် ပံ့ပိုးပေးထားပေမဲ့

[63] Sophia Cope, Amul Kalia, Seth Schoen, and Adam Schwartz, *Digital Privacy at the U.S. Border: Protecting the Data On Your Devices* (Electronic Frontiers Foundation, 2017), https://www.eff.org/files/2018/01/11/digital-privacy-border-12-2017.pdf

[64] Johana Bhuiyan, "How to protect your phone and data privacy at the US border," *The Guardian*, March 26, 2025, https://www.theguardian.com/technology/2025/mar/26/phone-search-privacy-us-border-immigration

အထူးသဖြင့်၊ ဖုန်းအဟောင်းတွေနဲ့ မကြာသေးခင်ကမှ ဆေး (reset)ထား တဲ့ ဖုန်းတွေမှာ ဒီလုပ်ဆောင်ချက်ကို ဖွင့်ထားခြင်း ရှိမရှိ အမြဲစစ်ဆေးသင့်ပါတယ်။

နယ်စပ်မှာဆိုရင် သင်ဟာ ဝင်ထွက်သွားလာခွင့်ရဖို့နဲ့ ခုခံကာကွယ်ဖို့ဆိုတဲ့ အချက်နှစ်ခုထဲက တစ်ခုကို ရွေးချယ်ရပါလိမ့်မယ်။ တချို့သူတွေဟာ ထပ်ပြီး ထိခိုက်နစ်နာမှု မရှိစေဖို့အတွက် လိုက်လျောညီထွေ လုပ်ဆောင်နိုင်သလို၊ တချို့ကတော့ သူတို့ရဲ့ ခြိမ်းခြောက်မှုအဆင့် (threat level) နဲ့ ဥပဒေရေးရာ အခြေအနေပေါ်မူတည်ပြီး ပြန်လည်ငြင်းဆန်တွန်းလှန်နိုင်ပါတယ်။ ဒီအခြေအနေအတွက် မှန်ကန်တဲ့ အဖြေဆိုတာ မရှိပါဘူး။ ဒါပေမဲ့ ဒီအချက်က ကျွန်တော်တို့ကို ပြောပြနေတာကတော့ သင့်ရဲ့ လုံခြုံရေးအစီအစဉ်ကို လေ့ကျင့် ဒါမှမဟုတ် သင်္ဘောပေါ် မတက်ခင်ကတည်းက စတင်ထားရမယ်၊ ပြီးတော့ သင်သယ်ဆောင်သွားတဲ့ အချက်အတိုင်းတိုင်းဟာ သင့်ရဲ့ ရွေးချယ်မှု ဖြစ်တယ်ဆိုတာပါပဲ။

ဇယား ၅- သင့်ရဲ့ မိုဘိုင်းလုံခြုံရေးအတွက် အထောက်အကူပြုနိုင်သော ကိရိယာများ (အားလုံးကို ဖော်ပြထားခြင်း မဟုတ်ပါ)

ကိရိယာ	**လုပ်ဆောင်ပေးချက်**	**ပလက်ဖောင်း**	**အင်တာနက်စာမျက်နှာ**	**မှတ်ချက်**
GrapheneOS	Google ဝန်ဆောင်မှုများ တွင် အလို အလျောက်မပါဝင်ဘဲ ပို ပြီးလုံခြုံ အောင် ၊ ကိုယ်ရေးကိုယ်တာ လုံခြုံမှု ကို အဓိကထားပြီး ဖန်တီး ထား တဲ့ Android စနစ်သုံး အမျိုး အစား ဖြစ်ပါတယ်။	Android (Pixel ဖုန်းအမျိုး အစားများသာ)	https://grapheneos.org/	Github eylenburg မှ သုံးစွဲသူ က Android စနစ်သုံး အမျိုးအစား အမျိုးမျိုးကို နှိုင်းယှဉ် ထား တဲ့ ပြည့်စုံတဲ့ ဇယား တစ်ခုကို ဖန်တီး ထားပါ တယ်။[65]
CalyxOS	အလွယ်တကူ တပ်ဆင်နိုင်ပြီး လုပ်နိုင်ပြီးကိုယ်ရေးကိုယ်တာ လုံခြုံမှုကိုလေးစားလိုက်နာတဲ့ A ndroid စနစ်သုံးအမျိုးအစား ဖြစ်ပါတယ်။ microG (Google ရဲ့ ဝန်ဆောင်မှု အစားထိုး) ကို လည်း ပံ့ပိုးပေးပါတယ်။	Android (ကန့်သတ်ဖုန်း မော်ဒယ်များအတွက်သာ)	https://calyxos.org/	
LineageOs	ကိုယ်ရေးကိုယ်တာလုံခြုံမှု အပိုင်မှာ GrapheneOS ထက် တော့ အားနည်းပါတယ်။ ဒါပေမဲ့ အခမဲ့ ဖြစ်ပြီး ၊ မည်သူမဆို ဝင်ရောက် နိုင်တဲ့	Android (ကန့်သတ်ဖုန်း မော်ဒယ်များအတွက်သာ)	https://lineageos.org/	

[65] eylenburg, "Comparison of Android-based Operating Systems," *Eylenburg.github.io* (blog), accessed June 15, 2025, https://eylenburg.github.io/os_comparison.htm.

	(open-source) ဖြစ်တဲ့ လုပ်ငန်းလည်ပတ်မှုစနစ် တစ်ခု ဖြစ်ပါတယ်။			
F-Droid	မည်သူမဆို ဝင်ရောက် နိုင်တဲ့ အပလီကေးရှင်း ထားရာနေရာ (Open-source app store)	Android	https://f-droid.org/	Google Play Store ကို အစားထိုး အသုံးပြုနိုင်တဲ့ အပလီကေးရှင်း ထားရာနေရာ တစ်ခု ဖြစ်ပါတယ်။
Aurora Store	Google Play အတွက် အခမဲ့ နှင့် မည်သူမဆို ဝင်ရောက် နိုင်တဲ့ (FOSS- Free and Open-Source Software) ဝန်ဆောင်မှုယူသူ		https://auroraoss.com/	အခြေခံအားဖြင့်တော့ ဒီဟာ က ခြေရာခံခြင်း မလုပ်တဲ့ Google Play ပါပဲ ။
AFWall+	အပလီကေးရှင်းတွေကို အင်တာနက်သုံးစွဲခွင့် မရအောင် ပိတ်ဆို့ပေးပါတယ်။	Android	https://github.com/ukanth/afwall	အခြေခံ ဝင်ရောက်ခွင့် (root access) လိုအပ် ပါတယ်။
NetGuard	အပလီကေးရှင်းတစ်ခုချင်းစီအတွက် အင်တာနက်သုံးစွဲခွင့်ကို ပိတ်ဆို့ပေးတဲ့ ကွန်ယက်လုံခြုံရေး ကိရိယာ (Firewall) ဖြစ်ပါတယ်။	Android	https://netguard.me/	အခြေခံ ဝင်ရောက်ခွင့် (root access) မလိုအပ်ပါ။
Shelter	သင့်ရဲ့ ကိုယ်ပိုင် နေရာကနေ အပလီကေးရှင်း တွေကို သီးခြားခွဲထုတ်ထားနိုင်ဖို့ အလုပ်နဲ့ပတ်သတ်တဲ့ကိုယ်ရေးအကျဉ်း (sandbox) တစ်ခုကို ဖန်တီးပေးပါတယ်။	Android	https://github.com/PeterCxy/Shelternet.typeblog.shelter/	
Scrambled Exif	ပုံတွေထဲက နောက်ဆက်တွဲ အချက်အလက် (Metadata) တွေကို ဖယ်ရှားပေး ပါတယ်။	Android	https://play.google.com/store/apps/details?id=com.jarsilio.android.scrambledeggsif&hl=en_AU	
Lockdown Privacy	iOS စနစ်သုံး စက်ပစ္စည်း တွေပေါ်ကဖုံးကွယ်ထားတဲ့ လှုပ်ရှားစောင့်ကြည့်တဲ့အရာ တွေကို ပိတ်ဆို့ပေးပါတယ်။	iOS	https://apps.apple.com/au/app/lockdown-privacy-vpn-proxy/id1469783711	

FUTO keyboard	ကိုယ်ရေးကိုယ်တာလုံခြုံမှုကို လေးစားလိုက်နာတဲ့ လက်ကွက် (Keyboard) အစားထိုး အပလီကေး ဖြစ်ပါတယ်။	Android	https://keyboard.futo.org/	
Heliboard	AOSP ကို အခြေခံထားပြီး ကိုယ်ရေးကိုယ်တာလုံခြုံမှုကို ဂရုစိုက်တဲ့ မည်သူမဆို ဝင်ရောက် နိုင်တဲ့ (open source) လက်ကွက် တစ်ခု ဖြစ်ပါတယ်။	Android	https://f-droid.org/en/packages/helium314.keyboard/	

ဆက်သွယ်မှု လုံခြုံရေး

ကျနော်တို့လုပ်ဆောင်သမျှအရာအားလုံးရဲ့ အဓိကအချက်က ဆယ်သွယ်ရေးပဲဖြစ်တယ်။ ဆက်သွယ်ရေးကနေတစ်ဆင့် ကျွန်တော်တို့ဟာ မဟာမိတ်ဖွဲ့တာ၊ လှုပ်ရှားမှုတွေ တည်ဆောက်တာ၊ ယုံကြည်မှု တည်ဆောက်တာ၊ ဗဟုသုတတွေ မျှဝေတာနဲ့ ဆော်ဩစည်းရုံးတာတွေကို လုပ်ဆောင်နိုင်ပါတယ်။ တက်ကြွလှုပ်ရှားသူတွေအနေနဲ့ ဒီလိုဆက်သွယ်ရတာကိုက ကျွန်တော်တို့ရဲ့ အားနည်းချက်တစ်ခုလည်း ဖြစ်စေပါတယ်။ အီးမေးလ်ဖြစ်စေ၊ စုဖွဲ့ဆွေးနွေးနိုင်တဲ့ ကွန်ယက် (group chat) ထဲက စာတစ်စောင်ဖြစ်စေ ကျွန်တော်တို့ ဘာပြောတယ်၊ ဘယ်လိုပြောတယ်၊ ဘယ်နေရာ၊ ဘယ်အချိန်မှာ ပြောတယ်ဆိုတာတွေဟာ အချက်အလက်စုဆောင်းခြင်း (data harvesting) ၊ စောင့်ကြည့်ခြင်း (surveillance) နဲ့ ဖျက်ဆီးပြောင်းလဲခြင်း (tampering) တို့ရဲ့ ခြိမ်းခြောက်မှုအောက်မှာ အမြဲရှိနေပါတယ်။ သင့်ရဲ့ ဆက်သွယ်ရေးလမ်းကြောင်းတွေ လုံခြုံမှုမရှိဘူးဆိုရင် သင့်ရဲ့ စုစည်းလှုပ်ရှားမှုတွေဟာလည်း လုံခြုံတယ်လို့ မဆိုနိုင်ပါဘူး။

ဒီအပိုင်းမှာ အီးမေးလ်နဲ့ ချက်ချင်း အချက်အလက်တွေဆက်သွယ်ဆောက်ရွက်ခြင်း နှစ်မျိုးလုံးအတွက် လုံခြုံတဲ့ ဆက်သွယ်ရေး ကိရိယာတွေကို အဓိကထား ဖော်ပြထားပါတယ်။ ဒီနေရာမှာ ဥပမာတချို့ကို တက်ကြွလှုပ်ရှားသူတွေက တက်ကြွလှုပ်ရှားသူအချင်းချင်းတွေအတွက် ဖန်တီးထားတာဖြစ်ပြီး၊ တချို့ကိုတော့ ကိုယ်ရေးကိုယ်တာ လုံခြုံမှု ကို အဓိကထားတဲ့ အဖွဲ့အစည်းတွေ ဒါမှမဟုတ် လွတ်လပ်တဲ့ တီထွင်ဖန်တီးသူတွေက ဖန်တီးထားတာ ဖြစ်ပါတယ်။ ဒါပေမဲ့ အရေးကြီးတာကတော့ ဒီ ကိရိယာတွေကို စာဝှက်လျှို့ဝှက်ကုဒ်စနစ် (encryption), ဗဟိုချုပ်ကိုင်မှုလျော့ချခြင်း (decentralisation) နဲ့ အသုံးပြုသူရဲ့ ထိန်းချုပ်မှု (user control) စတဲ့ မူဝါဒတွေပေါ် အခြေခံပြီး တည်ဆောက် ထားတာပဲ ဖြစ်ပါတယ်။ ဒါပေမဲ့ ဒီမှာကျွန်တော်တို့ ပြောခဲ့ပြီးသား အရာတွေလိုပဲ ဘယ် ကိရိယာ မှ ပြီးပြည့်စုံတာမျိုး မရှိပါဘူး။ သင့်ကို စောင့်ကြည့်ပြီး အမြတ်ထုတ်ဖို့ ရည်ရွယ်ပြီး ဒီဇိုင်းထုတ်ထားတဲ့ ကိရိယာတွေကို သုံးစွဲဖို့ ငြင်းဆန်ခြင်းအပေါ်မှာပဲ မူတည်ပါတယ်။ ဒီအပိုင်းဟာ

သင့်ရဲ့ လှုပ်ရှားမှုဆောက်ရွက်မှုတွေကို အချက်အလက်စုစည်းရာ (data point) တစ်ခုလို သဘောထားတဲ့ ပလက်ဖောင်း တွေအပေါ် သင့်ရဲ့ မှီခိုမှုကို ဖြတ်တောက်နိုင်ဖို့ အထောက်အကူပြုနိုင်ပါစေ။

အီးမေး

ဇယား ၆- သင်အစားထိုးအသုံးပြုနိုင်သော ကိုယ်ရေးကိုယ်တာလုံခြုံရေးကိုဦးစားပေးသော အီမေးဝန်ဆောင်မှုများ

ကိရိယာ	**လုပ်ဆောင်ပေးချက်**	**ပလက်ဖောင်း**	**F-droid ပလက်ဖောင်းတွင် ရှိ/မရှိ**	**အင်တာနက်စာမျက်နှာ**	**မှတ်စုများ**
Tuta	ဂျာမနီအခြေစိုက် အလုံးစုံစာဝှက်လျှို့ဝှက်ကုဒ်စနစ် သုံးတဲ့ အီးမေး (E2E encrypted email) ဖြစ်ပါတယ်။	Web, Android, iOS, desktop apps	ရှိ	https://tuta.com/	Tuta သည် PGP ကို အသုံးပြုခြင်း မရှိဘဲ၊ ၎င်း၏ကိုယ်ပိုင် လျှို့ဝှက်ကုဒ် အဖြစ်ပြောင်း လဲ ခြင်း (encryption) စနစ်ကို အသုံးပြုပါသည်။
Proton Mail	ဆွစ်ဇာလန်အခြေစိုက် အလုံးစုံစာဝှက်လျှို့ဝှက်ကုဒ်စနစ် သုံးတဲ့ အီးမေး (E2E encrypted email) ဖြစ်ပါတယ်။	Web, Android, iOS, desktop (via bridge)	မရှိ	https://proton.me/mail	ဆွစ်ဇာလန်နိုင်ငံဟာ အချက်အလက် ထိန်းသိမ်းထားရှိမှု (data retention) နဲ့ ပတ်သက်ပြီး အတင်းကြပ်ဆုံး ဥပဒေတွေ တစ်ခုကို ပိုင်ဆိုင်ထားပါတယ်။ သို့သော်လည်း ဒီလုံခြုံရေးဥပဒေကို ပြန်လည်ပြင်ဆင် ဖို့ စဉ်းစားနေပါတယ်။ အကယ်၍ ဒီဥပဒေကို အတည်ပြုလိုက်မယ်ဆိုရင် ဆွစ်ဇာလန်အခြေစိုက် ကုမ္ပဏီတွေ ဟာ အာဏာပိုင်တွေနဲ့ အချက်အလက်တွေ မျှဝေဖို့အတွက် ပူးပေါင်းဆောင် ရွက်ရပါလိမ့်မယ်[66]။ ဒါဟာ ကမ္ဘာ တစ်ဝန်းမှာ အခြေအနေ တွေ ဘယ်ဘက်ကို ဦးတည်နေသလဲ ဆိုတာကို ရှင်းလင်းစွာ ပြသနေတဲ့ အချက်တစ်ခု ဖြစ်ပါတယ်။
Mailbox.org	ဂျာမနီအခြေစိုက် စာဝှက်လျှို့ဝှက်ကုဒ်စနစ် သုံးတဲ့ အီးမေး	Web, standard clients (IMAP/SMTP)	မရှိ	https://mailbox.org/en/	

[66] Matt Jancer, “Proton Says It’ll Leave Switzerland if This Controversial Law Is Passed,” *Vice*, May 15, 2025, https://www.vice.com/en/article/proton-says-it-will-leave-switzerland-if-controversial-swiss-law-passes/

Riseup	PGP ပံ့ပိုးပေးထားတဲ့ တက်ကြွလှုပ်ရှားသူတွေ ဦးဆောင်တဲ့ စုပေါင်း အီးမေးဖြစ်ပါတယ်။	Web, standard clients (IMAP/SMTP)	မရှိ	https://riseup.net/en/email	ဖိတ်ကြားခြင်းခံရသူများအတွက်သာ
Posteo	ကောင်းမွန်သည့် ကိုယ်ရေးကိုယ်တာလုံခြုံမှု (PGP) ပံ့ပိုးပေးထားတဲ့ ဂျာမနီအခြေစိုက် အချက်အလက်တွေကို လျှို့ဝှက်ကုဒ် အဖြစ်ပြောင်း လဲခြင်း စနစ်သုံးတဲ့ အီးမေး	Web, standard clients (IMAP/SMTP)	မရှိ	https://posteo.de/en	(အမည်/နေရပ်လိပ်စာ မလိုအပ်ဘဲ) အမည်မဖော်ဘဲ အကောင့်ဖွင့်နိုင်ပါတယ်။
Disroot	ကောင်းမွန်သည့် ကိုယ်ရေးကိုယ်တာလုံခြုံမှု (PGP) ပံ့ပိုးပေးထားတဲ့ အခမဲ့ အီးမေး	Web, standard clients	မရှိ	https://disroot.org/en/services/email	
SimpleLogin	အီးမေးလ် လိပ်စာနာမည် အတုထုတ်ပေးခြင်း (emai aliasing) နဲ့ အီးမေးကို ပြန်လည်ပို့ပေးခြင်း (email forwarding) တို့ကို အသုံးပြုခြင်း။ သင့်ရဲ့ တကယ့်အီးမေးလ်ကို ကာကွယ်ဖို့အတွက် ယာယီအီးမေးလိပ်စာ (burner addresses)တွေ ဖန်တီးပေးသည်	Web, Android, iOS	မရှိ	https://simplelogin.io/	Proton Mail နဲ့ အပြည့်အဝ ပေါင်းစပ်အသုံးပြုနိုင်သလို၊ သီးခြားအနေနဲ့လည်း အသုံးပြုနိုင်ပါတယ်။
Addy.io	အီးမေးလ် လိပ်စာနာမည် အတုထုတ်ပေးခြင်း (emai aliasing) နဲ့ အီးမေးကို ပြန်လည်ပို့ပေးခြင်း (email forwarding)	Web	မရှိ	https://addy.io/	
Thunderbird	ကောင်းမွန်သည့် ကိုယ်ရေး ကိုယ်တာလုံခြုံမှု (PGP) မည်သူမဆို ဝင်ရောက် နှိုင်တဲ့ အချက်အလက် တွေကို	Windows, macOS, Linux	မရှိ	https://www.thunderbird.net/	

	လျှို့ဝှက်ကုဒ် အဖြစ် ပြောင်း လဲ ခြင်း စနစ်နဲ့ အီးမေးလ် လိပ်စာ နာမည် အတုထုတ်ပေးတဲ့ စနစ် ကို ပံ့ပိုးပေးထား တဲ့ မည်သူမဆို ဝင်ရောက် နိုင်တဲ့ (open-source) ကွန်ပျူတာ အီးမေး ဖောက်သည်(desktop email client)ဖြစ်ပါ တယ်။				
K-9 Mail	ကောင်းမွန်သည့် ကိုယ် ရေး ကိုယ်တာလုံခြုံမှု (PGP) ပံ့ပိုးပေးထားတဲ့ မည်သူမဆို ဝင်ရောက် နိုင်တဲ့ အီးမေး ဖောက်သည်	Android	ရှိ		

လုံခြုံစိတ်ချရသော စာ/အချက်အလက်ပေးပို့ခြင်း (Secure Messaging)

ဇယား ၇- သင်အစားထိုးအသုံးပြုနိုင်သော ကိုယ်ရေးကိုယ်တာလုံခြုံရေးကို ဦးစားပေးသော စာ/အချက်အလက်ပေးပို့ခြင်း ကိရိယာများ

ကိရိယာ	**လုပ်ဆောင်ပေးချက်**	**ပလက်ဖောင်း**	**F-droid ပလက်ဖောင်းတွင် ရှိ/မရှိ**	**အင်တာနက် စာမျက်နှာ**	**မှတ်စုများ**
Signal	အဆုံးမှအဆုံး အချက်အလက်တွေကို လျှို့ဝှက်ကုဒ် အဖြစ် ပြောင်းလဲ ခြင်း စနစ်သုံးတဲ့ စာတိုပေးပို့ခြင်း၊ အသံနဲ့ ဗီဒီယို ခေါ်ဆိုမှုများ။	Android, iOS, Desktop (linked to phone)	ရှိ	https://signal.org/	အကောင့်ဖွင့်ရန်အတွက် ဖုန်းနံပါတ်လိုအပ်ပါသည်။
Molly	Signal ကို အခြေခံထားပြီး လုံခြုံရေးဆိုင်ရာ လုပ်ဆောင်ချက် တွေကို ထပ် တိုးဖန်တီးထား တဲ့ လုံခြုံရေး တိုးမြှင့်ပေးတဲ့ ပိုမို လုံခြုံမှုရှိတဲ့	Android	ရှိ	https://molly.im/	ဖုန်းသော့ပိတ်ထားစဉ် အကာအကွယ်တွေ (lock screen protections) နဲ့ ကိုယ်ပိုင် ကုတ်စီမံခန့်ခွဲခြင်း(PIN handling) တို့လို

	အရာ (hardened fork) တစ်ခု ဖြစ်ပါတယ်။				မျိုး လုပ်ဆောင်ချက်တွေကို ထပ်တိုးထည့်သွင်းပေးပါ တယ်။
Element (Matrix)	Matrix ဗဟိုချုပ်ကိုင်မှု လျှော့ချထား သော ကွန်ရက် အတွက် လုံခြုံ စိတ်ချရသော စာတိုပေးပို့ရေး client ဖြစ်သည်။ ၎င်းသည် အလုံးစုံ စာဝှက်လျှို့ဝှက်ကုဒ်စနစ် (E2EE)၊ အဖွဲ့လိုက် စကားပြော ခန်းများနှင့် server ပေါင်းများ စွာတွင် ပေါင်းစည်းမှုကို ထောက်ပံ့ပေး သည် ။	Android, iOS, Web, Desktop	ရှိ	https://element.io/	
Jitsi	လျှို့ဝှက်ကုဒ်သုံးစနစ်၊ မျက်နှာပြင်မျှဝေခြင်း နဲ့ စာဖြင့် ဆက်သွယ်ပြောဆိုခြင်း တို့ကို ထောက်ပံ့ပေးတဲ့ မည်သူဆိုမ ဆိုလက်လှမ်းမှီသော (open-source) ဗီဒီယိုကွန်ဖရင့်	Web, Android, iOS	ရှိ	https://jitsi.org/	Jitsi ကို ကိုယ်တိုင် host လုပ်နိုင်ပါတယ် ။ သို့မဟုတ် https://meet.jit.si/ မှတဆင့်လည်း အသုံးပြုနိုင်ပါတယ်။ ဒါပေမယ့် အဲဒီ ဖြစ်စဉ် အတွက် ကတော့ Google ဒါမှမဟုတ် Microsoft နဲ့ အတည်ပြုချက်ယူဖို့ လိုအပ်ပါတယ်။ ကိုယ်တိုင် host လုပ်ပါ။
BigBlueButton	အွန်လိုင်းသင်ယူမှုနှင့် အဖွဲ့လိုက် ပူးပေါင်းဆောင်ရွက်မှု အတွက် ဒီဇိုင်းထုတ်ထားသော မည်သူဆိုမဆိုလက်လှမ်းမှီ သော (open-source) ဗီဒီယို ကွန်ဖရင့် ပလက်ဖောင်း	Web	မရှိ	https://bigbluebutton.org/	အသုံးပြုရလွယ်ကူခြင်း မရှိပါ။ (Not as plug-and-play)

စည်းရုံးရေးလှုံဆော်ရေး

ဇယား ၈- သင်အစားထိုးအသုံးပြုနိုင်သော ကိုယ်ရေးကိုယ်တာလုံခြုံရေးကို ဦးစားပေးသော စည်းရုံးလှုံဆော်ရေး ကိရိယာများ

ကိရိယာ	**လုပ်ဆောင်ပေးချက်**	**ပလက်ဖောင်း**	**F-droid ပလက်ဖောင်းတွင် ရှိ/မရှိ**	**အင်တာနက် စာမျက်နှာ**	**မှတ်စုများ**
Mobilizon	ကိုယ်ရေးကိုယ်တာလုံခြုံမှုကို အလေးထားတဲ့ Facebook events ရဲ့ အခြားရွေးချယ်စရာတစ်ခု ဖြစ်ပြီး ပွဲတွေကို ရှာဖွေနိုင်ခြင်း၊ ဖန်တီးနိုင်ခြင်းနဲ့ မျှဝေနိုင်ခြင်းတို့ လုပ်ဆောင်နိုင်ပါတယ် ။	Android, Web	ရှိ	https://mobilizon.org/#key-points	
Agorakit	အဖွဲ့အစည်းများအတွက် စီစဉ်ခြင်း၊ ဆွေးနွေးခြင်းနှင့် အချိန်ဇယားဆွဲ ခြင်းတို့ အတွက် ရည်ရွယ်သည့် မည်သူဆိုမဆိုလက်လှမ်းမှီသော (open-source) groupware.	Web	မရှိ	https://agorakit.org/en/	

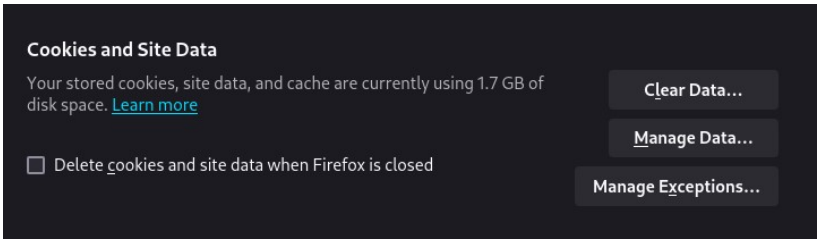
အင်တာနက် ဘရောက်ဇာများနဲ့ အွန်လိုင်း လုံခြုံရေး

ယနေ့ခေတ်လူတွေဟာ အင်တာနက် ဘရောက်ဇာတွေကို သတင်းအချက်အလက်ရှာဖွေဖို့၊ တက္ကစီခေါ်ဖို့၊ အစားအသောက် မှာယူဖို့နဲ့ အနီးဆုံးအများသုံးသန့်စင်ခန်းကို ရှာဖွေဖို့ စတဲ့နေ့စဉ်ဘဝ ကိစ္စရပ်တွေအတွက် တွင်တွင်ကျယ်ကျယ် အသုံးပြုနေကြပါတယ်။ လက်တွေ့မှာတော့ ကျွန်တော်တို့ရဲ့ ဘဝကဏ္ဍတိုင်းနီးပါးဟာ အင်တာနက်ဘရောက်ဇာတွေန ့ ဆက်နွယ်နေပါတယ်။ ဒါပေမယ ့် ဒီလိုအဆင်ပြေလွယ်ကူမှုတွေအတွက် ဘယ်လောက်တောင် အဖိုးအခကြီးကြီးနဲ့ ရင်းနှီးပေးဆပ်နေရသလဲဆိုတာကိုတော့ လူနည်းစုကသာ သတိပြုမိကြပါတယ်။ ကျွန်တော်တို့ရဲ့ ကလစ်တစ်ချက်၊ ဖွင့်လိုက်တဲ့ အင်တာနက်စာမျက်နှာတစ်ခု၊ ရှာဖွေမှုတစ်ခုနဲ့ ဘရောက်ဇာရဲ့ အခင်းအကျင်း (setting) တွေအားလုံးဟာ ကျွန်တော်တို့ကို ခြေရာခံဖို့နဲ့ အချက်အလက်တွေ စုဆောင်းဖို့ အသုံးပြုနိုင်တ ့ သတင်းအချက်အလက်တွေ ဖြစ်ပါတယ်။ ဥပမာအားဖြင့်၊ ဖန်သားပြင်ရဲ့ အရွယ်အစား၊ ပုံရိပ်တွေကို စက်တွကနေ ဘယ်လိုဖော်ပြလဲ၊ အချိန်ပိုင်းဇုန်နဲ့ ဘာသာစကားဆက်တင်တွေလို

မျိုး အပြစ်ကင်းတယ်လို့ ထင်ရတဲ့ ဆက်တင် တွေဟာတောင် ကျွန်တော်တို့အကြောင်း အသေးစိတ် အချက်အလက်တွေကို ဖန်တီးဖို့ အထောက်အကူဖြစ်စေပါတယ်။ ဒါကြောင့် ဘရောက်ဇာတွေနဲ့ အင်တာနက် အသုံးပြုတာဟာ ဟာ ကျွန်တော်တို့ အွန်လိုင်းမှာလုပ်နိုင်တဲ့ သတင်းအချက် အလက်အကြွယ်ဝဆုံးနဲ့ အန္တရာယ် အရှိဆုံး လုပ်ဆောင်မှုတွေထဲက တစ်ခုဖြစ်ပါတယ်။

အင်တာနက်စာမျက်နှာတွေက ဘယ်လို ခြေရာခံသလဲ

အင်တာနက်စာမျက်နှာတွေက သုံးစွဲသူတွေကို ခြေရာခံရာမှာ အစွမ်းအထက်ဆုံး နည်းလမ်းတစ်ခုကတော့ ဘရောက်ဇာ လက်ဗွေနှိပ်ခြင်း (browser fingerprinting) ဖြစ်ပါတယ်။ လူတွေက လက်ဗွေနှိပ်ခြင်းကို ကွတ်ကီး (cookies) တွေနဲ့ မကြာခဏ မှားတတ်ကြပေမယ့် သူတို့နှစ်ခုဟာ အခြေခံအားဖြင့် လုပ်ဆောင်ပုံချင်း မတူပါဘူး။ ကွတ်ကီး (Cookies) ဆိုတာကတော့ အင်တာနက်စာမျက်နှာတွေက သင်ရဲ့လုပ်ဆောင်ချက်တွေကို မှတ်မိနိုင်ဖို့ အတွက်သုံးတဲ့ သင့်စက်ထဲမှာ သိမ်းဆည်းထားတဲ့ ဖိုင်ငယ်လေးတွေပဲ ဖြစ်ပါတယ်။ အောက်ပါ နမူနာ Firefox ဘရောက်ဇာရဲ့ မျက်နှာပြင်ပုံမှာ ပြထားသလို ကွတ်ကီးတွေကို ရှင်းလင်းတာ၊ ပိတ်ဆို့တာတွေ ပြုလုပ်နိုင်ပါတယ်။ တစ်ဖက်မှာတော့ ဒစ်ဂျစ်တယ် လက်ဗွေနှိပ်ခြင်း (digital fingerprinting) ဟာ ကွတ်ကီးတွေထက် အများကြီး ပိုဆိုး ပါတယ်။



ဓာတ်ပုံရှင်းလင်းချက်- ဤပုံသည် Firefox ၏ "Cookies and Site Data" အခင်းအကျင်းများ ကဏ္ဍကို ရိုက်ကူးထားသည့် မျက်နှာပြင်ပုံဖြစ်သည်။ ၎င်းသည် သိမ်းဆည်းထားသော ကွတ်ကီးများ၊ ဆိုက်ဒေတာများနှင့် ကက်ရှ် (cache) များက လက်ရှိတွင် ဒစ်ဂျစ်တယ်နေရာ (disk space) ၁.၇ GB အသုံးပြုနေကြောင်း ဖော်ပြထားသည်။

Tuta အီးမေးက Hanna က လက်ဗွေနှိပ်ခြင်းရဲ့ အန္တရာယ်တွေနဲ့ Google က ဘာကြောင့် ဒီနည်းလမ်းကို အသုံးပြု ဖို့အလွန်စိတ်ဝင်စားရသလဲဆိုတာကို ရှင်းပြခဲ့ပါတယ်[67] ။ သူမရဲ့အဆိုအရ၊ ကွတ်ကီးတွေနဲ့မတူဘဲ ဒစ်ဂျစ်တယ် လက် ဗွေ နှိပ်ခြင်းဟာ မပျောက်ပျက်ဘဲ ဆက်ရှိနေပြီး ဖျက်လို့ ဒါမှမဟုတ် ရှင်းထုတ်လို့မရပါဘူး။ အင်တာနက်ဘရောက်ဆာ အသုံးပြုမှုမှတ်တမ်းတွေကို ရှင်းလင်းပြီးနောက်မှာတောင် သုံးစွဲသူတွေဟာ အင်တာနက်စာမျက်နှာတွေ၊ စက်တွေနဲ့ ဝန်ဆောင်မှုတွေ တစ်လျှောက် ခြေရာခံမှုကိုခံနေရဆဲ ဖြစ်ပါတယ်။ ဒစ်ဂျစ်တယ် လက်ဗွေနှိပ်ခြင်းဟာ လူတွေကို မည်သူမည်ဝါဖြစ်သည်ကို သတ်မှတ်ဖော်ထုတ်ဖို့အတွက် အင်တာနက်ပြင်ပမှ

[67] Hanna, “Digital Fingerprinting: Google launched a new era of tracking, but you can fight for your privacy!” Tuta, February 18, 2025, https://tuta.com/blog/digital-fingerprinting-worse-than-cookies

အသုံးပြုတဲ့ ဇီဝဆိုင်ရာ အချက်အလက် တွေကောက်တာနဲ့ ဆင်တူပါတယ်[68]။ အဲဒါကတော့ ထူးခြားတဲ့ အချက်အလက်တစ်ခု ဖြစ်ပေမယ့် ကျွန်တော်တို့ရဲ့ အင်တာနက် ပြင်ပမှ အသုံးပြုတဲ့ ဇီဝဆိုင်ရာအချက်အလက်တွေ ကောက်တာနဲ့မတူတာကတော့ ဒါဟာ သတင်းအချက် အလက်စုံမှတ် တစ်ခုတည်းအပေါ်မှာ မူတည်မနေပါဘူး။ ၎င်းဟာ သင့်စက်က အင်တာနက်စာမျက်နှာတွေကို ဖော်ပြပေးလိုက်တဲ့ ထူးခြားတဲ့ လက္ခဏာ ရပ်တွေပေါင်းစပ် မှု အပေါ်မှာ အခြေခံပါတယ်။ ဥပမာအားဖြင့်၊ သင့်ရဲ့ ဘရောက်ဇာ ဗားရှင်း၊ ကွန်ပျူတာ စနစ် (operating system)၊ ဖန်သားပြင်အရွယ်အစား (screen resolution)၊ ဖောင့်စနစ် (system fonts)၊ CPU ဗိသုကာလက်ရာ၊ WebGL ရုပ်ပုံဖော်စနစ် နဲ့ HTML5 canvas ကိုသုံးပြီး သင့်ဘရောက်ဇာက မမြင်နိုင်တဲ့ အစိတ်အပိုင်းတွေကို ဘယ်လိုပုံဖော်သလဲ ဆိုတာတွေ ပါဝင်ပါတယ်။

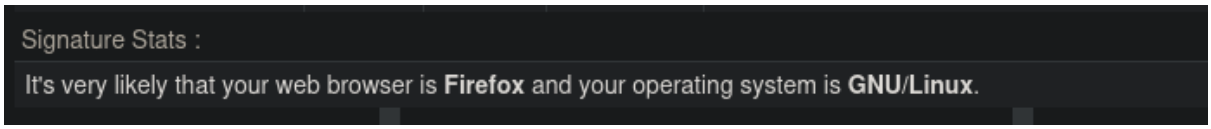
အီအက်ဖ်အက်ဖ် (EFF) ရဲ့ အင်တာနက်စာမျက်နှာဖြစ်တဲ့ သင်ရဲ့လှုပ်ရှားမှာတွေကို ဖုံကွယ်ပါ (Cover your tracks) (coveryourtracks.eff.org) ဟာ သင့်ရဲ့ အင်တာနက်ဘရောက်ဆာအသုံးပြုမှု ပုံစံတွေကို ဆန်းစစ်ရာမှာ ကူညီပေးပါတယ်။ ဒီစမ်းသပ်မှုကို ပြုလုပ်တဲ့အခါ သင့်အင်တာနက်ဘရောက်ဇာက ကြော်ငြာတွေကို ခြေရာခံခြင်း၊ မမြင်ရတဲ့ ခြေရာခံကိရိယာတွေ (invisible trackers) ကို ပိတ်ဆို့ခြင်း ရှိမရှိနဲ့ ထူးခြားတဲ့ ဒစ်ဂျစ်တယ်လက်ဗွေ (unique fingerprint) တစ်ခုကို ချန်ထားခဲ့ခြင်း ရှိမရှိဆိုတာကို စစ်ဆေးပေးပါတယ်။ သင့်ရဲ့ပန်းတိုင်ဟာ ကိုယ်ရေးကိုယ်တာလုံခြုံမှု (privacy) ဖြစ်တယ်ဆိုရင် ထူးခြားတဲ့ ဒစ်ဂျစ်တယ်လက်ဗွေ (unique fingerprint) ရှိတာဟာ ကောင်းတဲ့အရာတစ်ခု မဟုတ်ပါဘူး။ အင်တာနက်ဘရောက်ဆာတွေသုံးတဲ့အခါမှာ သင့်ရဲ့ရည်ရွယ်ချက်ဟာ တခြားသူတွေနဲ့ ရောနှောနေဖို့ ဖြစ်ပါတယ်။ ဒါ့ကြောင့် ကိုယ်ရေးကိုယ်တာလုံခြုံရေးကို အဓိကထားတဲ့ အင်တာနက်ဘရောက်ဇာအများစုဟာ ဘရောက်ဇာရဲ့ လုပ်ဆောင်မှုတွေကို စံနမူနာဖြစ်အောင် လုပ်ဆောင်ကြပါတယ်။ ဥပမာအားဖြင့်၊ ဝင်းဒိုး (Window) အရွယ်အစားကို 200px x 100px ရဲ့ အဆပေါင်းများစွာအဖြစ် သတ်မှတ်တာ၊ သင့်ရဲ့အချိန်ဇုန်ကို UTC အဖြစ် သတင်းပို့တာ ဒါမှမဟုတ် ပေါင်းစပ်အသုံးပြုနိုင်တဲ့ ဆော့ဖ်ဝဲ (add-ons သို့မဟုတ် extensions) တွေ မပါဝင်စေတာမျိုးတွေ ဖြစ်ပါတယ်။

ဒစ်ဂျစ်တယ် လက်ဗွေနှိပ်ခြင်းမှာ အမျိုးအစားများစွာရှိပေမယ့် ဒီလမ်းညွှန်မှာတော့ အသုံးအများဆုံးဖြစ်တဲ့ ကင်းဗပ်စ် (Canvas)၊ အော်ဒီယို (Audio) နဲ့ ဝက်ဘ်ဂျီအယ်လ (WebGL) လက်ဗွေနှိပ်ခြင်း သုံးမျိုးအကြောင်းကို အဓိကထား ရှင်းပြပါမယ်။ ကင်းဗပ်စ် လက်ဗွေနှိပ်ခြင်း (Canvas Fingerprinting) ဟာ သင့်အင်တာနက်ဘရောက်ဇာကို HTML5 <canvas> ကို အသုံးပြုပြီး မမြင်ရတဲ့ ပုံတစ်ပုံ ဒါမှမဟုတ် စာသားတစ်ခုကို ရေးဆွဲဖို့ ညွှန်ကြားခြင်းဖြင့် အလုပ်လုပ်ပါတယ်။ ဒီဖြစ်စဉ်ဟာ နောက်ကွယ်မှာ အလုပ်လုပ်တာကြောင့် သင့်မျက်နှာပြင်ပေါ်မှာ ဘာကိုမှမြင်ရမှာ မဟုတ်ပါဘူး[69]။ ကင်းဗပ်စ်ဟာ သင့်စက်က ဂရပ်ဖစ် (Graphics) ကို ဘယ်လိုကိုင်တွယ်တယ်ဆိုတဲ့ သေးငယ်တဲ့ ကွဲပြားမှု တွေကို စုဆောင်းပါတယ်။ ဥပမာအားဖြင့်၊ ဂျီပီယူ (GPU)၊

[68] Michael Crider, “Digital fingerprinting: The secret, insidious way you’re tracked online,” PcWorld, April 13, 2023, https://www.pcworld.com/article/1684308/what-is-a-digital-fingerprint.html

[69] “Canvas fingerprinting: what is is and how it works,” Fingerprint, accessed June 17, 2025, https://fingerprint.com/blog/canvas-fingerprinting/

anti-aliasing အခင်းအကျင်းများ၊ စာလုံးပုံဖော်ခြင်း (font rendering) နဲ့ သင့်ကွန်ပျူတာစနစ် (OS) အကြောင်း အချက်အလက်တွေ ပါဝင်ပါတယ်။ ကင်းဗပ်စ် လက်ဗွေနှိပ်ခြင်း (Canvas Fingerprinting) ဟာ သင့်စနစ်က ပစ်ဆယ်လ် (pixels) တွေကို ဘယ်လိုရေးဆွဲသလဲဆိုတဲ့ အချက်အလက်တွေကို တိုက်ရိုက်ရယူတာ ဖြစ်လို့ ကွတ်ကီး (cookies) တွေ ဒါမှမဟုတ် သိုလှောင်မှု (storage) ကို အသုံးပြုဖို့ မလိုအပ်ပါဘူး။ ဥပမာအနေနဲ့၊ ကျွန်တော် လက်ရှိအသုံးပြုနေတဲ့ စက်အကြောင်း ဘာတွေသိလဲဆိုတာ သိရှိနိုင်ဖို့ browserleaks.com အင်တာနက်စာမျက်နှာကို သွားခဲ့ရာမှာ အောက်ပါအတိုင်း တွေ့ရှိခဲ့ရပါတယ်။



ဓာတ်ပုံရှင်းလင်းချက်- ဤပုံသည် ဘရောက်ဆာ၏ လက်ဗွေရာကို ခြေရာခံခြင်းဆိုင်ရာ တွေ့ရှိမှု ရလဒ်များကို ပြသထားသည့် ဖန်သားပြင်ပုံ ဖြစ်သည်။ "Signature Stats: It's very likely that your web browser is Firefox and your operating system is GNU/Linux." ဟူသော မက်ဆေ့ချ်တွင် "သင့်၏ ဝက်ဘ်ဘရောက်ဆာမှာ Firefox ဖြစ်နိုင်ပြီး သင့်၏ ကွန်ပျူတာစနစ်မှာ GNU/Linux ဖြစ်နိုင်ခြေ အလွန်များပါသည်။" ဟု ဖော်ပြထားသည်။

တစ်ဖက်မှာ အသံ လက်ဗွေနှိပ်ခြင်း (Audio fingerprinting) ကတော့ အင်တာနက် အသံ API (Web Audio API) ကိုသုံးပြီး သင့်စက်ရဲ့ အသံထုတ်လုပ်မှုစနစ် (audio processing stack) ကို အသံတိတ် အသံတစ်ခု ပေးပို့ခြင်းဖြင့် အလုပ်လုပ်ပါတယ်။ ၎င်းဟာ API ရဲ့ AudioContext interface အင်တာဖေ့စ်ကို အသုံးချပြီး အသံကို အင်တာနက် ဘရောက်ဇာထဲမှာ တိုက်ရိုက်ဖန်တီး၊ ခွဲခြမ်းစိတ်ဖြာပါတယ်။ သင်က အင်တာနက်စာမျက်နှာတစ်ခုကို ဝင်ရောက် ကြည့်ရှုတဲ့အခါ အသံတိတ်အသံတစ်ခုကို ဖွင့်ပေးပြီး အဲဒီအသံဟာ သင့်စက်ရဲ့ အသံစနစ်တစ်လျှောက် ဖြတ်သန်း သွားပါတယ်။ စက်ပစ္စည်းတိုင်းသည် အသံကို ကိုယ်ပိုင်နည်းလမ်းများဖြင့် သီးခြားစီ စီမံဆောင်ရွက်သောကြောင့် သင့်ကဲ့သို့ တူညီသော စက်ပစ္စည်းမျိုး အသုံးပြုသူ ရှိနေလျှင်ပင် ရလဒ်ထွက်ပေါ်လာသည့် အသံသည် သင့် အတွက် သီးသန့်ဖြစ်နေတဲ့ လက်ဗွေရာကဲ့သို့ ဖြစ်နေပါသည်[70]။

နောက်ဆုံးအနေနဲ့၊ WebGL လက်ဗွေနှိပ်ခြင်း (WebGL fingerprinting) ဟာ သင့်စက်က မြေပုံတွေ၊ ဂိမ်းတွေ ဒါမှမဟုတ် ရုပ်ပုံဆိုင်ရာ အထူးပြုလုပ်ချက်တွေ လိုမျိုး သုံးဖက်မြင် ဂရပ်ဖစ်ပုံစံတွေ (3D graphics) ကို ဘယ်လိုပုံဖော်တယ်ဆိုတာကို ခြေရာခံပါတယ်[71]။ တစ်ဖက်မှာတော့ အသံ လက်ဗွေနှိပ်ခြင်းနဲ့ ဆင်တူစွာ၊ သင့်စက် ရဲ့ ဟာ့ဒ်ဝဲနဲ့ ဆော့ဖ်ဝဲ အခင်းအကျင်း (setting) တွေမှာရှိတဲ့ သေးငယ်တဲ့ ကွဲပြားမှုတွေကတောင် ဒီဂရပ်ဖစ်တွေ ပုံဖော်ပုံအပေါ် သက်ရောက်မှုရှိပါတယ်။ ဒါကြောင့် အင်တာနက်စာမျက်နှာတစ်ခုက WebGL လက်ဗွေနှိပ်

[70] "What is Audio fingerprint," Datadome, accessed June 17, 2025, https://datadome.co/anti-detect-tools/audio-fingerprint/

[71] "WebGL Fingerprint," Multilogin, accessed June 17, 2025, https://multilogin.com/glossary/webgl-fingerprint/

ခြင်းကို အသုံးပြုတဲ့အခါ သင့်အင်တာနက်ဘရောက်ဇာကို သီးခြားပုံသဏ္ဌာန် ဒါမှမဟုတ် ပုံရိပ်တစ်ခုကို ပုံဖော်ခိုင်းပြီး ရရှိလာတဲ့ ရလဒ်ကို တိုင်းတာပါတယ်။

ဒစ်ဂျစ်တယ် လက်ဗွေနှိပ်ခြင်း (Fingerprinting) ဟာ လူတွေကို စောင့်ကြည့်ဖို့အတွက် မကောင်းတဲ့၊အန္တရာယ်ရှိတဲ့ နည်းလမ်းတစ်ခုဖြစ်ပါတယ်။ ဘာလို့လဲဆိုတော့ ဘရောက်ဆာနဲ့ အင်တာနက်သုံးဖို့ ကျွန်တော်တို့ လိုအပ်တဲ့အရာ တွေဟာ သတင်းအချက်အလက်ဆုံမှတ်တွေ ဖြစ်သွားလို့ပါပဲ။ ဒစ်ဂျစ်တယ် လက်ဗွေနှိပ်ခြင်း အကြောင်း ပြောကြတဲ့အခါ Librefox ဆိုတဲ့ ဘရောက်ဇာကို မကြာခဏဆိုသလို ကြားရတတ်ပါတယ်။ Librefox ဟာ Firefox ကိုအခြေခံပြီး ဖန်တီးထားတဲ့ ကိုယ်ရေးကိုယ်တာလုံခြုံရေးကို အထူးအာရုံစိုက်တဲ့ အင်တာနက်ဘရောက်ဇာတစ်ခု ဖြစ်ပါတယ်။ ဒါဟာ သတင်းအချက်အလက်တွေကို အလိုအလျောက် စုဆောင်း၊ မျှဝေ၊ ခွဲခြမ်းစိပ်ဖြာမှုလုပ်ငန်းစဉ် (telemetry) တွေကို ဖြုတ်ပစ်ပြီး လက်ဗွေနှိပ်ခြင်းကို ကာကွယ်ဖို့အတွက် အခင်းအကျင်း (setting) တွေကို ပိုမိုတင်း ကျပ်ကာ ခြေရာခံကိရိယာတွေ အသုံးချနိုင်တဲ့ လုပ်ဆောင်ချက်များ စွာကိုလည်း ပိတ်ထားပေးပါတယ်။ ကျွန်တော် (Jean) ဟာ Librefox ကို အရင်က သုံးဖူးပြီး အခုထိလည်း သုံးနေဆဲမို့ ကျနော့်စက်ထဲမှာတပ်ဆင်ထားဆဲပါ။ ဒါပေမယ့် ဒီအင်တာနက်ဘရောက်ဇာရဲ့ လုံခြုံရေးက အခက်အခဲအချို့နဲ့ လာပါတယ်။ ဥပမာအားဖြင့်၊ အင်တာနက်မီဒီယိုတွေ ကြည့်မရတာ ဒါမှမဟုတ် လုံးဝမတက်လာတာမျိုး ကြုံဖူးပါတယ်။ အချိန်ဇုန်နဲ့ပတ်သက်ပြီး သုံးရတာလည်း ခက်ခဲပါတယ်။ ဘာလို့လဲဆိုတော့ အင်တာနက်စာမျက်နှာတွေက အချိန်ဇုန်အချက်အလက်ကို လက်ဗွေနှိပ်ခြင်းအတွက် မသုံးနိုင်အောင် သူက အဲဒီအချက်အလက်ကို ပိတ်ဆို့ထားလို့ပါပဲ။ သို့ပေမယ့်လည်း ကျွန်တော့်ရဲ့ ခြိမ်းခြောက်မှုအန္တရာယ်အဆင့်ကတော့ ဒီလိုစိတ်အနှောင့်အယှက်ဖြစ်စရာတွေကို လက်ခံနိုင် ပါတယ်။ လူတိုင်းကတော့ ဒီလောက်အထိ တင်းကျပ်တဲ့ လုံခြုံရေးမျိုး မလိုအပ်ပါဘူး။ တစ်ချို့သူတွေအတွက် အသုံးပြုရလွယ်ကူမှုက ပိုအရေးကြီးပြီး တစ်ချို့အတွက်ကတော့ အဆင်ပြေမှုထက် လုံခြုံရေးကို ဦးစားပေးကြပါတယ်။ သင့်ရဲ့ Firefox အင်တာနက်ဘရောက်ဇာမှာ privacy.resistFingerprinting ဆက်တင်ကို ဖွင့်မဖွင့်ဆို တာကတော့ သင့်အပေါ်မှာပဲ မူတည်ပါတယ်။ ကျွန်တော့်ရဲ့ ခြိမ်းခြောက်မှုအန္တရာယ်အဆင့်အတွက်တော့ uBlock Origin လောက်နဲ့တင် လုံလောက်ပါတယ်။ နောက်ဆုံးအဓိကအရေးကြီးတာကတော့ ကိုယ့်ရဲ့အခြေအနေကို သိရှိနားလည်ပြီး ကိုယ့်နဲ့ကိုက်ညီမှုမရှိတဲ့ အခင်းအကျင်း တွေကို မျက်စိမှိတ် မှန်းဆပြီး ကူးချတာမျိုးမဟုတ်ဘဲ ရည်ရွယ်ချက်ရှိရှိ ရွေးချယ်တတ်ဖို့ပါပဲ။

လုံခြုံစိတ်ချရသော အင်တာနက်ဘရောက်ဇာများ

ဒီအပိုင်းမှာတော့ သင့်ရဲ့ ကိုယ်ရေးကိုယ်တာလုံခြုံမှုကို ဦးစားပေးတဲ့ အင်တာနက်ဘရောက်ဇာတွေနဲ့ ရှာဖွေရေးအင်ဂျင် တွေရဲ့ စာရင်းကို ဖော်ပြပေးသွားမှာဖြစ်ပါတယ်။ ဒီစာရင်းဟာ ပြည့်စုံလုံလောက်မှု မရှိနိုင်ပါဘူး။ ဘာလို့လဲဆိုတော့ ပြီးပြည့်စုံတဲ့ ဘရောက်ဇာ ဒါမှမဟုတ် ရှာဖွေရေးအင်ဂျင်ဆိုတာ မရှိပါဘူး။ ဒါပေမယ့် သင့်ရဲ့ ဒစ်ဂျစ် တယ်အလေ့အကျင့် တွေကို ဗဟိုချုပ်ကိုင်မှုလျော့ချလေ (de-centralise) နဲ့ GAFAM (Google, Apple,

Facebook, Amazon, Microsoft) ကို ရှောင်ရှားလေလေ၊ အာဏာပိုင်တွေအတွက် သင့်ကို စောင့်ကြည့်ဖို့ ပို ခက်ခဲလာ လေပါပဲ။

ဇယား ၉ - စည်ရုံးလှုံဆော်ရေးအတွက် သင်အသုံးပြုနိုင်သော ကိုယ်ရေးကိုယ်တာလုံခြုံရေးကို ဦးစားပေးသော ဘရောက်ဆာများ

ကိရိယာ/အပလီကေးရှင်း	**လုပ်ဆောင်ပေးချက်**	**ပလက်ဖောင်းများ**	**F-droid ပလက်ဖောင်းတွင် ရှိ/မရှိ**	**အင်တာနက်စာမျက်နှာ**	**မှတ်စုများ**
LibreWolf	သတင်းအချက်အလက်တွေကို အလိုအလျောက် စုဆောင်း၊ မျှဝေ၊ ခွဲခြမ်းစိပ်ဖြာမှု လုပ်ငန်းစဉ် (telemetry) ကို ဖယ်ရှားထားပြီး ကိုယ်ရေးကိုယ်တာလုံခြုံရေးအတွက် မူရင်းအခင်းအကျင်းများကို ထည့်သွင်းပေး ထားသည့် အပြင် uBlock Origin ကိုပါ ထည့်သွင်းပေးထားသော Firefox ၏ ပိုမိုလုံခြုံသည့် ပုံစံတစ်ခုဖြစ်သည်။	Linux, Win, macOS (via Homebrew)	မရှိ	https://librewolf.net/	
Fennec	လုံခြုံရေး ပိုမိုကောင်းမွန်အောင် ထပ်မံပြုပြင် ထားသည့် Firefox ပုံစံဖြစ်သော်လည်း သုံးစွဲသူများကို ခြေရာခံနိုင်သည့် Mozilla ဝန်ဆောင်မှုအချို့နှင့် ဆက်သွယ်နေဆဲ ဖြစ်သည်။	Android	ရှိ	https://f-droid.org/en/packages/org.mozilla.fennec_fdroid/	
Tor Browser	Tor ကွန်ရက်ကိုအသုံးပြုပြီး အင်တာနက်အသုံးပြုမှု မှတ်တမ်းများကို ဖုံးကွယ်ပေးပါသည်။	Linux, windows, macOS, android	ရှိ (Android)	https://www.torproject.org/	
Mullvad Browser	Mullvad VPN နှင့် Tor Project တို့မှ ဖန်တီး ထားသည့် ကိုယ်ရေးကိုယ်တာလုံခြုံ ရေးကို အထူးအာရုံစိုက်သောဘရောက်ဇာ ဖြစ် သည်။ ၎င်းသည် လက်မွေနှိပ်ခြင်းနှင့် ခြေရာခံခြင်းတို့ကို ဖယ်ရှားပေးပြီး ကိုယ်ပိုင် ကွန်ယက်အတု (VPN) နှင့်ဖြစ်စေ၊ ကိုယ်ပိုင် ကွန်ယက်အတု (VPN) မပါဘဲဖြစ်စေ အသုံးပြုရန် ရည်ရွယ်ထုတ်လုပ်ထားပါသည်။	Windows, macOS, Linux	No	https://mullvad.net/en/browser	
DuckDuckGo Search	အသုံးပြုသူများ၏ ရှာဖွေမှုမှတ်တမ်းကို သိမ်းဆည်းခြင်း သို့မဟုတ် ခြေရာခံခြင်း မပြုလုပ်သည့် ရှာဖွေရေးအင်ဂျင် (search engine) ဖြစ်ပါသည်။	Web, Android, iOS (browser version also available)	ရှိ (the browser)	https://duckduckgo.com/	
SearXNG	ကိုယ်တိုင်လက်ခံဆောင်ရွက်ပြီး (self-hosted)၊ မည်သူဆိုမဆို ဝင်ရောက်နိုင်သော (open-source) ဖြစ်သော ရှာဖွေရေးအင်ဂျင် (metasearch engine) တစ်ခုဖြစ်သည်။	Web (self-hosted or via public instances)		https://searxng.github.io/	

မြေပုံများ

လမ်းကြောင်းပြကိရိယာများသည် လူအများစု သယ်ဆောင်ထားသည့် အန္တရာယ်အရှိဆုံး စောင့်ကြည့်ရေးနည်းလမ်းများ ထဲမှ တစ်ခုဖြစ်သည်။ Google Maps ကဲ့သို့သော ကြီးမားသည့် မြေပုံဝန်ဆောင်မှုများသည် သင်ရွေ့လျားသွားလာသည့် နေရာတိုင်းကို အစမှအဆုံး ခြေရာခံပြီး နေရာတစ်ခုနှင့်တစ်ခုကြား အချိန်မည်မျှကြာသည်ကို မှတ်တမ်းတင်ထား ပါသည်။ ထို့ပြင် သင်၏ရှာဖွေမှုမှတ်တမ်းများ၊ တည်နေရာများနှင့် လမ်းကြောင်းမှတ်တမ်းများကိုလည်း မှတ်တမ်းယူ ထားပါသည်။ ကံကောင်းစွာဖြင့်၊ သင့်ကိုယ်ရေးကိုယ်တာလုံခြုံမှုကို လေးစားသည့် မြေပုံဝန်ဆောင်မှု အပလီကေးရှင်း များလည်း ရှိပါသည်။ ၎င်းကိရိယာများသည် OpenStreetMap မှ အချက်အလက်ကို အသုံးပြုထားပြီး ခြေရာခံခြင်းကို ရှောင်ရှားကာ အင်တာနက်မလိုဘဲလည်း အလုပ်လုပ်နိုင်ပါသည်။ ယင်းကဲ့သို့သော အပလီကေးရှင်းများကို အသုံးပြုရန် အချိန်အနည်းငယ်ယူရသော်လည်း ကြီးမားသောနည်းပညာကုမ္ပဏီများအပေါ် သင်၏ မှီခိုမှုကို ပိုမိုလျော့မြန်စွာ လျှော့ချနိုင်လေ၊ သင်၏ ဒစ်ဂျစ်တယ်ဘဝကို ပိုမိုလျင်မြန်စွာ ပြန်လည်ထိန်းချုပ်နိုင်လေ ဖြစ်ကြောင်း သတိရပါ။ ခုခံကာကွယ်မှုတိုင်းလိုပဲ ကြိုးစားအားထုတ်မှု လိုအပ်သော်လည်း ရလဒ်ကတော့ တန်ဖိုးရှိလှပါသည်။

ဇယား ၁၀- စည်ရုံးလှုံဆော်ရေးအတွက် သင်အသုံးပြုနိုင်သော ကိုယ်ရေးကိုယ်တာလုံခြုံရေးကို ဦးစားပေးသော မြေပုံများ

ကိရိယာ/အပလီကေးရှင်း	လုပ်ဆောင်ပေးချက်	**ပလင်ဖောင်း**	F-droid ပလက်ဖောင်းတွင် ရှိ/မရှိ	အင်တာနက်စာမျက်နှာ	**မှတ်စုများ**
Organic Maps	OpenStreetMap ကိုအခြေခံထားသည့် မည်သူဆိုမဆိုဝင်ရောက်နိုင်သော (open-source) မြေပုံအပလီကေးရှင်းတစ်ခု ဖြစ်သည်။ ကြော်ငြာမပါ၊ ခြေရာခံခြင်းမရှိ၊ သတင်းအချက် အလက်တွေကို အလိုအလျောက် စုဆောင်း၊ မျှဝေ၊ ခွဲခြမ်းစိပ်ဖြာမှု လုပ်ငန်းစဉ် (telemetry) လည်း မပါဝင်ဘဲ အင်တာနက်မလိုဘဲ လမ်းကြောင်းပြခြင်းကို လုပ်ဆောင် နိုင်သည်။	Android, iOS	ရှိ	https://organicmaps.app/	အင်တာနက်မလိုဘဲသုံးရန် အလွန်ကောင်းမွန်သည်။ ပေါ့ပါးပြီး၊ နည်းပညာနားမလည်သူများပင် အလွယ်တကူ အသုံးပြုနိုင်သည်။ စက်ဘီးစီး ခြင်း၊ လမ်းလျှောက် ခြင်းနှင့် ကားမောင်းခြင်း လမ်းကြောင်းများကို ထောက်ပံ့ပေးသည်။

OsmAnd	GPX ခြေရာခံခြင်း၊ မြေပုံစိတ်ကြိုက် ပြင်ဆင်ခြင်းနှင့် အင်တာနက်မလိုဘဲ လမ်းကြောင်းရှာဖွေခြင်းကဲ့သို့သော အဆင့်မြင့် လုပ်ဆောင်ချက်များ ပါဝင်သည့် မည်သူဆိုမဆိုဝင်ရောက်နိုင်သော (open-source) မြေပုံနှင့် လမ်းကြောင်းပြအက်ပ် တစ်ခု ဖြစ်ပါသည်။	Android, iOS	ရှိ	https://osmand.net/	Organic Maps ထက် လုပ်ဆောင်ချက်များ ပိုမိုစုံလင်သည်။ အလွှာ (layer) များဖြင့် မြေပုံကြည့်လိုသူများ သို့မဟုတ် plugin ထည့်သွင်း အသုံးပြုလိုသူများကဲ့သို့သော အဆင့်မြင့်အသုံးပြုသူများအတွက် သင့်တော်သည်။

စက်ပစ္စည်း လုံခြုံရေး (Device Security)

စက်ပစ္စည်း လုံခြုံရေးသည် ဒစ်ဂျစ်တယ်လုံခြုံရေးအားလုံး၏ အခြေခံအုတ်မြစ် ဖြစ်သည်။ ရုပ်ပိုင်းဆိုင်ရာအရ ထိတွေ့ခွင့်ရရှိခြင်း (physical access) သည် အစွမ်းအထက်ဆုံး တိုက်ခိုက်မှုနည်းလမ်းတစ်ခု ဖြစ်နေဆဲဖြစ်ရာ စက်ပစ္စည်းလုံခြုံရေးဆိုသည်မှာ ချိုးဖောက်ခံရခြင်းမှ လုံးဝကာကွယ်နိုင်ရန် သို့မဟုတ် တိုက်ခိုက်မှုကို စုံစမ်းထောက် လှမ်းရန်နှင့် တုံ့ပြန်ရန်အတွက် အချိန်အလုံအလောက်ရအောင် တားဆီးရန်အတွက် အတားအဆီးများ တည်ဆောက် ထားခြင်းကို ဆိုလိုသည်။ သော့ခတ်ထားခြင်းမရှိသော သို့မဟုတ် ကုဒ်ဝှက်မထားသော ခိုးယူခံရသည့် သို့မဟုတ် သိမ်းဆည်းခံရသည့် ဖုန်းတစ်လုံးသည် သိမ်းဆည်းသူ သို့ ခိုးယူသွားသူကို အချက်အလက်များစွာ ပေးအပ်နိုင်သည်။ ဒစ်ဂျစ်တယ်ကာကွယ်မှုများ ရှိနေသည့်တိုင်၊ ခေတ်နောက်ကျနေသော ဆော့ဖ်ဝဲ၊ အားနည်းသော စကားဝှက်များ သို့မဟုတ် အချက်များစွာဖြင့် စစ်မှန်ကြောင်း အတည်ပြုခြင်း (Multi-Factor Authentication) မရှိခြင်းတို့သည် တိုက်ခိုက်ခံရဖို့ လမ်းဖွင့်ပေးထားသလို ဖြစ်နေသည်။ စက်ပစ္စည်းလုံခြုံရေးသည် ဒီလမ်းညွှန်ရဲ့ နောက်ပိုင်းတွင်ဆွေးနွေးမည့် အင်တာနက်တစ်ကိုယ်ရေသန့်ရှင်းရေး (cyberhygiene) နှင့်လည်း ဆက်စပ်နေသည်။ ၎င်းကို တစ်ကြိမ်တည်း သတ်မှတ်ထားရုံဖြင့် မလုံလောက်ဘဲ အမြဲမပြတ် မွမ်းမံမှုများ (updates) ပြုလုပ်ရန် လိုအပ်သည်။ ကောင်းမွန်သော စက်ပစ္စည်း လုံခြုံရေးသည် ကောင်းမွန်သော ဆိုက်ဘာတစ်ကိုယ်ရေသန့်ရှင်းရေးကို အထောက်အကူပြုသည်။

ဤနေရာတွင် အဓိကအခန်းကဏ္ဍမှ ပါဝင်သည်မှာ စစ်မှန်ကြောင်း အတည်ပြုခြင်း (authentication) ဖြစ်ပြီး၊ ၎င်းသည် သင်သည် မည်သူမည်ဝါဖြစ်ကြောင်း သက်သေပြသည့် လုပ်ဆောင်ချက်ဖြစ်သည်။ ၎င်းသည် အဓိကအမျိုးအစား သုံးခု ပေါ်တွင် အခြေခံသည်။ ၎င်းတို့မှာ သင်သိသောအရာ (something you know) ၊ သင့်တွင်ရှိသော အရာ(something you have) ၊ သင်ကိုယ်တိုင် (something you are)။ လုံခြုံစိတ်ချရသော စစ်မှန်ကြောင်း အတည်ပြု ခြင်းသည် (authentication) အနည်းဆုံး အဆိုပါအချက်များထဲမှ နှစ်ခုကို ပေါင်းစပ်ထားပြီး ၎င်းကို အချက်များစွာဖြင့် စစ်မှန်ကြောင်း အတည်ပြုခြင်း (Multi-Factor Authentication - MFA) ဟု ခေါ်

ဆိုသည်။ အချက်များစွာဖြင့် စစ်မှန်ကြောင်း အတည်ပြုခြင်း (MFA) သည် အချက်တစ်ချက် ပေါက်ကြားသွားလျှင်တောင် ခွင့်ပြုချက်မရှိဘဲ ဝင်ရောက်အသုံးပြုခြင်း၏ အခွင့်အလမ်းကို လျော့ချပေးသည်။

MFA နှင့် 2FA

အဆင့်နှစ်ဆင့်ဖြင့် အတည်ပြုခြင်း (Two-Factor Authentication - 2FA) ဆိုသည်မှာ သင်၏ မည်သူမည်ဝါ ဖြစ်ကြောင်း သက်သေပြရန်အတွက် မတူညီသည့် နည်းလမ်းနှစ်ခု လိုအပ်သော လုံခြုံရေး (login) စနစ်တစ်ခုကို ရည်ညွှန်းသည်။ အချက်များစွာဖြင့် စစ်မှန်ကြောင်း အတည်ပြုခြင်း (Multi-Factor Authentication - MFA) တွင်မူ အဆိုပါအချက်နှစ်ခု သို့မဟုတ် နှစ်ခုထက်ပို၍ (multi ဆိုသည့် စကားလုံးအတိုင်း) ပါဝင်သည်။ ဥပမာအားဖြင့်၊ အချက်များစွာဖြင့် စစ်မှန်ကြောင်း အတည်ပြုခြင်း (MFA) တွင် စကားဝှက် (password)၊ လုံခြုံရေးသော့ (security key) သို့မဟုတ် လက်ဗွေစစ်ဆေးခြင်းတို့ ပါဝင်နိုင်သည်။

လက်ပ်တော့ပ်နှင့် ကွန်ပျူတာများ

ကြီးမားသောနည်းပညာ ကော်ပိုရေးရှင်းတွေဟာ ဖက်ဆစ်ဝါဒ ရုံးခန်းထဲမရောက်ခင်ကတည်းက ဒူးထောက်အညံ့ခံနေ တယ်ဆိုတဲ့ သတင်းတွေကြောင့် ကိုယ်ပိုင်အမှတ်တံဆိပ် စနစ်တွေနဲ့ စီးပွားဖြစ်ထုတ်လုပ်ထားတဲ့ ကိရိယာတွေကို အားကိုးခြင်းဟာ ဆွဲဆောင်မှု လျော့နည်းနည်းလာပါတယ်။ အထူးသဖြင့် တက်ကြွလှုပ်ရှားသူတွေနဲ့ ခုခံတော်လှန်ရေးလုပ်ငန်းတွေမှာ ပါဝင်နေသူတွေအားလုံးနီးပါအတွက်ဆို ပိုလို့တောင် ဆိုးရွားပါတယ်။ Microsoft ရဲ့ (Recall feature) လိုမျိုး စီးပွားဖြစ်ထုတ်လုပ်ထားတဲ့ ကိရိယာအများစုမှာ ပါဝင်နေတဲ့ ဗဟို ချုပ်ကိုင်မှုနဲ့ စောင့်ကြည့်နိုင်စွမ်းတွေဟာ အကျိုးရှိတာထက် အန္တရာယ်ပိုများလာစေပါတယ်[72]။

ဒစ်ဂျစ်တယ်လွတ်လပ်မှု (digital autonomy) ရရှိဖို့အတွက် ထိရောက်မှုအထိရောက်ဆုံး ခြေလှမ်းတွေထဲက တစ်ခုကတော့ Linux-based လုပ်ငန်းလည်ပတ်ရေး စနစ်ကို ပြောင်းလဲအသုံးပြုခြင်းပဲ ဖြစ်ပါတယ်။ Linux ဖြန့်ချိမှု (distribution) တစ်ခုစီမှာ သုံးစွဲရလွယ်ကူမှု မတူညီတာကြောင့် သင်ရွေးချယ်တဲ့ ဖြန့်ချိမှုအပေါ်မူတည်ပြီး သင်ယူလေ့လာရမယ့်အဆင့်တွေ ကွာခြားနိုင်ပါတယ်။ အကြောင်းအမျိုးမျိုးကြောင့် ချက်ချင်းပြောင်းလဲဖို့ မဖြစ်နိုင်ဘူး ဆိုရင်တော့ ကွန်ပြူတာသုံး ဓာတ်ပြား တစ်ခုလုံးကို အလုံးစုံစာဝှက်လျှို့ဝှက်ကုဒ်စနစ်သုံးခြင်း (full-disk encryption) ဟာ သင့်အတွက် အကောင်းဆုံးအဖော်ဖြစ်ပါလိမ့်မယ်။ ဒါ့အပြင် သင်မလိုအပ်တဲ့ ဆော့လ်ဝဲ (bloatware) သို့မဟုတ် အပလီကေးရှင်း တွေကို ဖယ်ရှားသင့်ပါတယ်။ Brock Bingham က Windows 11 မှာ မလိုအပ်ဘဲ ကြိုတင်ထည့်သွင်းထားတဲ့ အပလီကေးရှင်း တွေကို ဘယ်လိုခွဲခြားသိမြင်ရမလဲ ဆိုတာကနေစပြီး ၎င်းတို့ကို ဖယ်ရှားတဲ့ လုပ်ငန်းစဉ်အထိ ရှင်းလင်း စွာ အသေးစိတ်ဖော်ပြထားပါတယ်[73]။

---

[72] Imran Rahman-Jones, “Microsoft rolls out AI screenshot tool dubbed 'privacy nightmare,” *BBC News*, April 11, 2025, https://www.bbc.com/news/articles/cj3xjrj7v78o.

[73] Brock Bingham, “How to identify and remove bloatware from Windows 11,” *PDQ*, December 24, 2024, https://www.pdq.com/blog/how-to-remove-bloatware/

Microsoft ဟာ Windows 11 ထည့်သွင်းတဲ့အခါ Microsoft အကောင့်ထည့် သွင်းဖို့ လိုအပ်ချက်ကို ရှောင်ရှားတဲ့နည်းလမ်းကို မကြာသေးမီက ပိတ်ဆို့ခဲ့ပေ မယ့် SHIFT+F10 နည်းလမ်းကတော့ အခုထိ အလုပ်လုပ်နေဆဲ ဖြစ်တယ်လို့ အသုံးပြု သူတွေက တွေ့ရှိခဲ့ကြပါတယ်[74]။

နောက်ထပ် အကြံပြုချက်တစ်ခုကတော့ ဖြစ်နိုင်ရင် သင်ရဲ့ကိုယ်ပိုင်ဘဝနဲ့ တတ်ကြွလှုပ်ရှားစည်းရုံးရေးလုပ်ငန်းတွေကို မရောထွေးမိဖို့ပါပဲ။ ဆိုလိုတာကတော့ သင့်ရဲ့ အရေးကြီးတဲ့လုပ်ငန်းတွေအတွက် သီးသန့်စက်ပစ္စည်းတစ်ခုကို အသုံးပြုပြီး အချက်အလက်တွေကို ချိတ်ဆက်မှု (syncing) မလုပ်ထားဖို့ ဖြစ်ပါတယ်။ နောက်ဆုံးအနေနဲ့၊ ပြောနေကျ စကားဖြစ်ပေမယ့် သင့်ရဲ့အိမ်မွေးတိရစ္ဆာန်အမည် (သို့မဟုတ်) သင့်ရဲ့မွေးနှစ်ကို စကားဝှက်အဖြစ် အသုံးပြုတာဟာ မလုံခြုံပါဘူး။ သင့်စက်ပစ္စည်းရဲ့ လုံခြုံရေးကို စဉ်းစားတဲ့အခါ ထည့်သွင်းစဉ်းစားနိုင်တဲ့ ကိရိယာတွေရဲ့ စာရင်းကို (အပြည်အစုံမဟုတ်ပေမယ့်) အောက်မှာဖော်ပြထားပါတယ်။ သင်ထပ်ပေါင်းထည့်လိုက်တဲ့ လုံခြုံရေးအလွှာတိုင်းဟာ အောင်ပွဲတစ်ခုပါပဲ။

ဇယား ၁၁- စက်ပစ္စည်း လုံခြုံရေးအတွက် အထောက်အကူပြုနိုင်သော ကိရိယာများ (မပြည့်စုံသေးပါ)

ကိရိယာ	**လုပ်ဆောင်ပေးချက်**	ပလက်ဖောင်း	အင်တာနက်စာမျက်နှာများ	မှတ်စုများ
BitLocker/ FileVault/ LUKS	OS ကွန်ပျူတာစနစ် (OS) ထဲမှာ တည်ဆောက်ပြီးသားကွန်ပြူတာသုံး ဓာတ်ပြား တစ်ခုလုံးကို အလုံးစုံစာဝှက်လျှို့ဝှက်ကုဒ်စနစ် သုံးခြင်း (Full-disk encryption)	Win macOS, Linux		ဒါတွေကတော့ ကွန်ပျူတာစနစ် (OS) ထဲမှ ာ တည်ဆောက်ပြီး သား ကုဒ်ဝှက်စနစ် ဆော့ဖ်ဝဲတွေ ဖြစ်ပါတယ်။
VeraCrypt	ဖိုင်တွဲများ (folders)၊ အကန့်များ (partitions) သို့မဟုတ် ဒရိုက် (Drive)တစ်ခုလုံးကို ကုဒ်ဝှက်ပေးနိုင်သော ပြင်ပကုမ္ပဏီ၏ ကုဒ်ဝှက်စနစ် ဆော့ဖ်ဝဲ တစ်ခုဖြစ်သည်။	Linux, Win, macOS	https://www.veracrypt.fr/en/Downloads.html	
USBGuard	USB ကိရိယာများအား ခွင့်ပြုချက် ပေးခြင်းဆိုင်ရာ မူဝါဒ များကို အကောင်အထည်ဖော်ဆောင်ရွက်ပေးပါသည်။	Linux	https://usbguard.github.io/	
Little Snitch	သင့် Mac ကွန်ပျူတာသည် အင်တာနက်ပေါ်ရှိ မည်သည့် နေရာများနှင့် ချိတ်ဆက်နေသည်ကို ပြသပေးပါသည်။	macOS	https://www.obdev.at/products/littlesnitch/index.html	
OpenSnitch	သင်ထည့်သွင်းထားသည့် အပလီကေးရှင်းများမှ ပြုလုပ်သော အင်တာနက် တောင်းဆိုမှုများကို ခြေရာခံ ပေးပါသည်။	Linux	https://github.com/evilsocket/opensnitch	Linux အတွက် Little Snitch နှင့် တူညီသော ဆော့ဖ်ဝဲ
Prey	သင့်ရဲ့လက်ပ်တော့ပ် သို့မဟုတ် ဖုန်း အခိုးခံရပါက စက်ပစ္စည်းကို ခြေရာခံခြင်း၊	Linux, Win, macOS,	https://preyproject.com/	

[74] Jason Bagnell, "NO Microsoft Account Needed! Windows 11 Setup Bypass (LATEST 6/2025)" June 05, 2025, YouTube, https://www.youtube.com/watch?v=SiDLgdbFdtM.

	လော့ခ်ချခြင်းနှင့် အချက်အလက်များအား အဝေးမှ ဖျက်ပစ်ခြင်းတို့ ပြုလုပ်နိုင်သည်။	Android		
Find My Device	သင့် Windows 10 သို့မဟုတ် Windows 11 စက်ပစ္စည်း ပျောက် ဆုံးသွားခြင်း သို့မဟုတ် အခိုးခံ ရခြင်းတို့ ဖြစ်ပေါ်ပါက ၎င်း၏ တည်နေရာကို ရှာဖွေရာ တွင် ကူညီပေးနိုင်ပါသည်။	Win	https://account.microsoft.com/devices	
Find My	Find My Device ၏ macOS ဗားရှင်းဖြစ်ပါသည်။	macOS	https://support.apple.com/en-au/guide/icloud/mmfc0f0c67/1.0/icloud/1.0	
DoNotSpy11	Windows 11 အတွက် သူလျှို ကာကွယ်ရေးကိရိယာ ဖြစ်ပါသည်။	Win	https://pxc-coding.com/donotspy11/	
SDelete	ဖျက်လိုက်ပြီးသား ဖိုင်တွေကို ပြန်လည်ရေးသား ဖျက်ဆီးပေး ပါသည်။	Win	https://docs.microsoft.com/en-us/sysinternals/downloads/sdelete	

စကားဝှက် စီမံခန့်ခွဲမှု

ဇယား ၁၂- ကိုယ်ရေးကိုယ်တာလုံခြုံရေးကို ဦးစားပေးသော စကားဝှက် စီမံခန့်ခွဲမှု ကိရိယာများ

ကိရိယာ	**လုပ်ဆောင်ပေးချက်**	ပလက်ဖောင်း	အင်တာနက်စာမျက်နှာများ	မှတ်စုများ
Bitwarden	မည်သူဆိုမဆိုလက်လှမ်းမှီသော စကားဝှက် စီမံခန့်ခွဲရေး ဆော့ဖ်ဝဲလ် ဖြစ်ပြီး ခိုင်မာသော စကားဝှက်များ ကို သိမ်းဆည်းပေးခြင်း၊ ဖန်တီးပေး ခြင်းတို့ ပြုလုပ်နိုင်သည်။ ထို့ပြင် ကိရိယာအမျိုးမျိုးတွင် လျှို့ဝှက်ကုဒ် ဖြင့် ကာကွယ်ထားသော သိုလှောင် ခန်းများကို ချိတ်ဆက်ပေး ခြင်း (ကိုယ်တိုင်လည်ပတ်လိုပါက ရွေးချယ်နိုင်သည်) ကိုလည်း ပံ့ပိုး ပေးသည် ။	Linux, Win, macOS, Android, iOS, web	https://bitwarden.com/	
1Password	စကားဝှက်များ၊ ခရက်ဒစ်ကတ်များနှင့် ဆော့ဖ်ဝဲလ်လိုင်စင်များကို သိမ်းဆည်းနိုင်သော စကားဝှက် စီမံခန့်ခွဲရေး ဆော့ဖ်ဝဲလ် ။	Linux, Win, macOS, Android, iOS, web	https://1password.com/	
Proton Pass	Proton Mail ကို ဖန်တီးသူများက ပြုလုပ်ထားသော စကားဝှက် စီမံခန့်ခွဲရေး ဆော့ဖ်ဝဲလ် ဖြစ်ပြီး ဆော့ဖ်ဝဲလ်ထုတ်လုပ်သူ ဒါမှမဟုတ် ဝန်ဆောင်မှုပေးသူ ကိုယ်တိုင်ကတောင်မှ အသုံးပြုသူရဲ့ လျှို့ဝှက်အချက်အလက်တွေကို လုံးဝမသိရှိနိုင်ပါ ။	Linux, Win, macOS, Android, iOS, web	https://proton.me/pass	
KeePassXC	ကိုယ်ပိုင်ကွန်ပျူတာပေါ်မှာ အင်တာနက်ပြင်ပ (Offline) သိုလှောင်ထားနိုင်တဲ့ မည်သူဆိုမဆိုလက်လှမ်းမှီသော ဒေသတွင်း စကားဝှက် စီမံခန့်ခွဲရေး ဆော့ဖ်ဝဲလ်	Linux, Win, macOS	https://keepassxc.org/	
Yubikey	အားကောင်းသော အဆင့်နှစ်ဆင့်ဖြင့် အတည်ပြုခြင်း (two-factor authentication (2FA)) အတွက် စက်ပိုင်းဆိုင်ရာ ပစ္စည်း	Win, Linux, macOs	https://www.yubico.com/	စကားဝှက် စီမံခန့်ခွဲရေး ဆော့ဖ်ဝဲလ်မဟုတ်သော်လည်း, စက်ပိုင်းဆိုင်ရာ ပစ္စည်း ကိရိယာ လုံခြုံရေး သော့

	ကိရိယာ (Hard-ware) လုံခြုံရေးသော့			(hardware keys) များသည် TOTP ကုတ်များ ကို လုံခြုံစွာ ထုတ်ပေးရန်နှင့် စီမံခန့်ခွဲရန် အသုံးပြုနိုင် ပါသည်။
Nitrokey	မည်သူဆိုမဆိုလက်လှမ်းမှီသော စက်ပိုင်းဆိုင်ရာ ပစ္စည်းကိရိယာ (Hard-ware) လုံခြုံရေးသော့	Win, Linux, macOs	https:// www.nitrokey.com/	အထက်ပါ ဖော်ပြချက်နှင့်တူညီသည် ။

လုံခြုံစိတ်ချရသော သိုလှောင်မှု (Secure storage)

ဇယား ၁၃- ကိုယ်ရေးကိုယ်တာလုံခြုံရေးကို ဦးစားပေးသော လုံခြုံစိတ်ချရသော သိုလှောင်မှု ရွေးချယ်စရာများ

ကိရိယာ	**လုပ်ဆောင်ပေးချက်**	**ပလက်ဖောင်း**	**အင်တာနက်စာမျက်နှာများ**	**မှတ်စုများ**
CryptPad	ပေါင်းစပ်ထားသော စာရွက်စာတမ်းတည်းဖြတ်ခြင်း၊ ဖိုင်သိုလှောင်ခြင်း၊ မှတ်စုများ၊ ဇယားများနှင့် စစ်တမ်းများအတွက် လျှို့ဝှက်ကုဒ်ဖြင့် ထိန်းသိမ်းထားခြင်း	Web-based (browser)	https:// cryptpad.org/	
Proton Drive	အဆုံးမှအဆုံး အချက်အလက်တွေကို လျှို့ဝှက်ကုဒ် အဖြစ်ပြောင်းလဲခြင်း စနစ်သုံးတဲ့ cloud ဖိုင်သိုလှောင်မှု	Web, Android, iOS	https://proton.me/ drive	Proton Drive မှာ အခုဆိုရင် document feature တစ်ခု ပါလာပါပြီ။
Syncthing	မိမိကိုယ်ပိုင် ကိရိယာများအကြား peer-to-peer ဖိုင်များ တစ်ပြိုင်နက် တည်း အလုပ်လုပ်ခြင်း	Linux, Win, macOs	https:// syncthing.net/	
Nextcloud	ကိုယ်တိုင်လည်ပတ်သော ဖိုင်များအား တစ်ပြိုင်နက်တည်း အလုပ်လုပ်ပြီး မျှဝေနိုင်သည့် ပလက်ဖောင်း	Windows, macOS, Linux, Android, iOS	https:// nextcloud.com/	
Backblaze	စက်တစ်ခုလုံး(လက်တော့ပ်/ကွန်ပျူတာ) အတွက် လျှို့ဝှက်ကုဒ်ဖြင့် ထိန်းသိမ်းထားသော cloud အရန်သိမ်းဆည်းမှု။ အလိုအလျောက်နှင့် ဆက်တိုက် အရန်သိမ်းဆည်းမှုများကို အဓိကထားသည်။	Windows, macOS	https:// www.backblaze.com/	

Filen	အဆုံးမှအဆုံး အချက်အလက်တွေကို လျှို့ဝှက်ကုဒ် အဖြစ်ပြောင်းလဲခြင်း စနစ်သုံးတဲ့ cloud ဖိုင်သိုလှောင်မှု နှင့် ဖိုင်မျှဝေမှု။ ဆော့ဖ်ဝဲလ်ထုတ်လုပ်သူ ဒါမှမဟုတ် ဝန်ဆောင်မှုပေးသူ ကိုယ်တိုင်ကတောင်မှ အသုံးပြုသူရဲ့ လျှို့ဝှက် အချက်အလက်တွေကို လုံးဝမသိရှိနိုင်ပါ ။	Web, Linux, Android, iOS, Windows, macOS	https://filen.io/	

အပိုင်းသုံး: အစုအဖွဲ့လိုက် လွတ်မြောက်ရေး

စနစ်တကျ ဖိနှိပ်မှုများနှင့် အာဏာရှင်အင်အားစုနဲ့ အရင်ရှင်းတို့၏ ကမ္ဘာလုံးဆိုင်ရာ ဒစ်ဂျစ်တယ်စစ်ပွဲများ အောက်တွင် ရှင်သန်ရပ်တည်နိုင်ရေးသည် တစ်ဦးချင်းစီ၏ ကြိုးပမ်းမှုသက်သက် မဖြစ်နိုင်ပါ။ ဤအခန်းတွင် ခုခံတော်လှန်ရေး အတွက် စုစည်းထားသော လူအဖွဲ့အစည်းများက လွတ်မြောက်ရေးတိုက်ပွဲကို ရှေ့ဆက်နိုင်ရန် အတွက် ကြံခိုင်သော စောင့်ရှောက်မှု၊ လုံခြုံရေးနှင့် နိုင်ငံရေးအင်အားစုများကို မည်သို့တည်ဆောက်နိုင် ကြောင်း ဆွေးနွေးထားပါသည်။ လူအများပြောလေ့ရှိသကဲ့သို့ စုပေါင်းညီညွတ်မှုတွင် လုံခြုံမှုရှိသည်။ ထို့ကြောင့် အုပ်ချုပ်သူလူတန်းစားများက ဖိနှိပ်ရန်၊ ကွဲပြားအောင်လုပ်ဆောင်ရန်နှင့် အတိုက်အခံဆန့်ကျင်သူများကို တိတ်ဆိတ်သွားစေရန် ပိုမိုအသုံးချလာသည့် ကမ္ဘာကြီးတွင် နှိပ်စက်ညှဉ်းပန်းမှုများနှင့် ရင်ဆိုင်နေရသော ရဲဘော်များအား ရှင်သန်ရပ်တည်ရေးနှင့် စည်းလုံးညီညွတ် ရေးအတွက် လိုအပ်သော ကိရိယာများကို တပ်ဆင် ပေးရန် လိုအပ်ကြောင်း ကျွန်ုပ်တို့ အသိအမှတ်ပြုပါသည်။

ဤအခန်းတွင် လှုပ်ရှားတက်ကြွသူများ၊ စည်းရုံးလှုံဆော်သူများနှင့် ရှေ့တန်းမှ လုပ်ဆောင်နေသူများအနေဖြင့် နှောင့်ယှက်မှုများ၊ စောင့်ကြည့်မှုများနှင့် ကိုယ်ရေးကိုယ်တာလုံခြုံမှု ချိုးဖောက်ခံရခြင်းတို့ကို ခုခံကာကွယ်ရန် အသုံးပြု နိုင်သည့် နည်းဗျူဟာများကို ဖော်ပြထားပါသည်။ ကျွန်ုပ်တို့သည် အကြမ်းဖက်အစိုးရများ၊ အမြတ် ထုတ်သော ကော်ပို ရေးရှင်းများနှင့် ဖောက်ပြန်ရေးအင်အားစုများ၏ ပစ်မှတ်ထားခြင်းခံရသူများအပေါ်တွင်သာ ကာကွယ်ရေးန့ဲ ပတ်သတ် ပြီး လုံးလုံးလျားလျား တာဝန်ရှိသည်ဟူသော အယူအဆကို ပယ်ချပါသည်။ အဘယ်ကြောင့်ဆိုသော် ထိုသို့သော ယုတ္တိဗေဒသည် စနစ်တကျအကြမ်းဖက်မှုကို တစ်ဦးချင်းစီ၏ ပြဿနာ အဖြစ် ပုံဖော်ကာ ၎င်းကို ဖြစ်ပေါ်စေသည့် ဖွဲ့စည်းတည်ဆောက်ပုံဆိုင်ရာ (Structural) အခြေအနေများမှ အာရုံ လွဲသွားစေသောကြောင့် ဖြစ်ပါသည်။

ကျွန်တော်တို့ရဲ့ ရည်ရွယ်ချက်ကတော့ အာဏာကို စိန်ခေါ်ပြောဆိုတာကြောင့် အနိုင်ကျင့်ခံနေရတဲ့၊ နှိပ်စက် ညှဉ်းပန်းခံ နေရတဲ့သူတွေကို အထောက်အကူပြုဖို့ ဖြစ်ပါတယ်။ ဒါဟာ သူတို့ရဲ့ ကောင်းကျိုး၊ သူတို့ရဲ့ အသက် အိုးအိမ်စည်းစိမ်နဲ့ အရေးအကြီးဆုံးဖြစ်တဲ့ လွတ်မြောက်ရေးနဲ့ တရားမျှတမှုအတွက် တိုက်ပွဲဝင်နေတဲ့ လှုပ်ရှားမှု တွေရဲ့ ကျယ်ပြန့်တဲ့ ဂုဏ်သိက္ခာကို ကာကွယ်ဖို့ ကူညီနိုင်တဲ့ ကိရိယာတွေနဲ့ လုပ်ငန်းစဉ်တွေကတစ်ဆင့် ပေါ်ထွက် လာတာပါ။ အင်အားကြီးလာတဲ့ ဖက်ဆစ်အစိုးရတွေနဲ့ အတိုက်အခံတွေကို တိုက်ခိုက်ဖို့အတွက် ဒစ်ဂျစ်တယ် အခြေခံ အဆောက်အအုံတွေကို လက်နက်အဖြစ် အသုံးပြုနေတာတွေကြောင့် အရပ်ဘက်လူအဖွဲ့အစည်းတွေ ဟာ စုပေါင်း ကာကွယ်ရေးအတွက် လမ်းညွှန်ချက်တွေနဲ့ ကိရိယာတွေကို တီထွင်ဖို့ စုစည်းလှုပ်ရှားခဲ့ကြပါတယ်။ ဒီစာမျက်နှာတွေဟာ ဒီလိုကြိုးပမ်းအားထုတ်မှုတချို့ကို မှတ်တမ်းတင်ထားတာ ဖြစ်ပါတယ်။

ဒစ်ဂျစ်တယ် တစ်ကိုယ်ရေသန့်ရှင်းမှုနှင့် လုံခြုံသော အလေ့အထများ တည်ဆောက်ခြင်း

တစ်ချိန်က အဆင့်အတန်းခွဲခြားမှုများကို ဖျက်သိမ်းပေးမည့် ကြီးမားသော တန်းတူညီမျှရေး ကိရိယာတစ်ခုဟု ကတိပြုခဲ့သည့်အရာသည် ယခုအခါ လူတန်းစားတိုက်ပွဲ၏ ရှေ့တန်းစစ်မျက်နှာတစ်ခု ဖြစ်လာခဲ့သည်[75]။ယနေ့ခေတ်မှာ ကျွန်တော်တို့ရဲ့ အရင်းနှီးဆုံး စကားပြောဆိုမှုတွေနဲ့ အပြန်အလှန် ဆက်ဆံမှုတွေတောင်မှ ဒေါ်လာဆိုတဲ့ နာမည်တစ်ခုဖြစ်တဲ့ ငွေကြေးအတွက် ကုန်ပစ္စည်းသဖွယ် အမြတ်ထုတ်ခံနေရတဲ့ ကမ္ဘာကြီးမှာ နေထိုင်နေ ကြရပါတယ်။ ဒီလိုမျိုး အမြတ်ထုတ်မှုက ငွေကြေးအသုံးပြုပြီး လွတ်လပ်မှုနဲ့ လုံခြုံမှုကို ဝယ်ယူနိုင်တဲ့ ရှေးဟောင်းစနစ်ကို ပိုပြီးခိုင်မာ စေပါတယ်။ ဒီလိုအခြေအနေမှာ ကိုယ်ရေးကိုယ်တာလုံခြုံရေးသည် ဇိမ်ခံပစ္စည်းတစ်ခု ဖြစ်လာပြီး လုံခြုံရေးဆိုတာ လည်း တတ်နိုင်သူများအတွက်သာ ရရှိနိုင်သည့် အရာတစ်ခု ဖြစ်လာခဲ့သည်။

ဒစ်ဂျစ်တယ် သို့မဟုတ် ဆိုက်ဘာ တစ်ကိုယ်ရေသန့်ရှင်းမှု (Digital or cyber hygiene) ဟာ ကျွန်တော်တို့လက်ထဲမှာ ကျန်ရှိနေသေးတဲ့ ကိရိယာအနည်းငယ်ထဲက တစ်ခုဖြစ်ပါတယ်။ ဒီလမ်းညွှန်ရဲ့ အရင်အပိုင်းတွေမှာ ဖော်ပြခဲ့တဲ့ တခြားနည်းလမ်းတွေ၊ ကိရိယာတွေလိုပဲ ဆိုက်ဘာတစ်ကိုယ် ရေသန့်ရှင်းမှုဟာ အပြီးသတ်ဖြေရှင်းနိုင်တဲ့ အရာတစ်ခု၊ လွတ်မြောက်မှု အတွက် လည်း မဟုတ်ပါဘူး။ ဒါပေမယ့် ဒါဟာ စတင်နိုင်မယ့်အရာ တစ်ခု ဖြစ်ပါတယ်။ ဒါဟာ ကျွန်တော်တို့ရဲ့ ခန္ဓာကိုယ်၊ မည်သူမည်ဝါဖြစ်ကြောင်းဖော်ထုတ်ပေးနိုင်တဲ့ ကိုယ်ပိုင်အချက်အလက် နဲ့ ကိုယ့်ရဲ့ကျန်ရှိနေ သေးတဲ့ အစိတ်အပိုင်းတွေကို ထိန်းချုပ်နိုင်ဖို့အတွက် နည်းလမ်းတစ်ခုပါပဲ။ ကမ္ဘာတစ်ဝန်းရှိ ဖိနှိပ်မှုဆန့်ကျင်ရေး လှုပ်ရှားသူတွေရဲ့ ကွန်ရက်တစ်ခုဖြစ်တဲ့ Blueprints for Change ဟာ ဒစ်ဂျစ်တယ်လုံခြုံရေး အခြေခံအချက်များ (Digital Security Basics) ကို ဖော်ပြထားပါတယ်။ အဲဒီအချက်တွေကတော့ အန္တရာယ်အဆင့် နည်းပါးကနေ အလယ်အလတ်ရှိသူတွေအတွက် လိုက်နာနိုင်တဲ့ အဆင့်တွေပဲ ဖြစ်ပါတယ်။[76]

- ကွန်ပျူတာနဲ့ အခြားစက်ပစ္စည်းတွေမှာ သင်ရဲ့ OS၊ အင်တာနက်ဘရောက်ဇာနဲ့ အပလီကေးရှင်းတွေကို အဆင့်မြှင့်တင်မှု (Update) လုပ်ထားပါ။
- သင်အသုံးပြုတဲ့ (cloud) ဝန်ဆောင်မှုတိုင်းအတွက် အချက်များစွာဖြင့် စစ်မှန်ကြောင်း အတည်ပြုခြင်း (Multi-Factor Authentication (MFA)) ကို ဖွင့်ထားပါ။
- ဆစ်ကနယ် (Signal) နဲ့ Jitsi ကို အသုံးပြုပါ။
- စကားဝှက်တွေကို ပိုမိုခိုင်မာအောင် ဖန်တီးဖို့ စကားဝှက်မန်နေဂျာ (password manager) ကို အသုံးပြုပါ။

[75] Nicholas Negroponte, *Being Digital*, 1st Edition. (Knopf, 1995), 243

[76] Blueprints for Change, *How-to Draft: Digital Security Basics for Campaigners* (Blueprints for Change, 2018), https://docs.google.com/document/d/1skNzkvS3NcdDeHqzguOI6FfWxuCsOsKyCl8c8aNxzY8/edit?tab=t.0

- အရာအားလုံးကို ကုဒ်ဝှက်ထားပါ။
- flash drive နဲ့ hard drive တွေကို သတိထားပါ။
- သင့်စက်ပစ္စည်းတွေကို လုံခြုံအောင်ထားပါ။

ဒစ်ဂျစ်တယ် တစ်ကိုယ်ရေသန့်ရှင်းမှု ကို တစ်ဦးချင်းစီရဲ့ ပြဿနာတစ်ခုအဖြစ် မမြင်သင့်ပါဘူး။ ဘာလို့လဲဆို တော့ ဒါဟာ တစ်ဦးချင်းစီရဲ့ ပြဿနာမဟုတ်ဘဲ စုပေါင်းပြဿနာ ဖြစ်ပြီး စုပေါင်းဖြေရှင်းမှု လိုအပ်လို့ပါ။ လက်တွေ့မှာ သင်လုပ်ဆောင်တဲ့အရာတွေဟာ တခြားသူတွေရဲ့ အချက်အလက်တွေကိုပါ သက်ရောက်မှုရှိပါ တယ်။ ဒါ့ကြောင့် လစ်ဘရယ်တွေရဲ့ ကိုယ်ရေးကိုယ်တာလုံခြုံမှု အခွင့်အရေးအပေါ် အမြင်ဟာ အခြေခံအားဖြင့် ကို မှားယွင်းနေတာပါ။ သူတို့က ကိုယ်ရေးကိုယ်တာလုံခြုံမှုကို တစ်ကိုယ်ရေပိုင်ဆိုင်ခွင့်တစ်ခု၊ ကိုယ်ပိုင်အရာ တစ်ခု၊ ပြုသမျှနုသောအရာတစ်ခု၊ သို့မဟုတ် ရှိခြင်း၊ မရှိခြင်းသက်သက်အဖြစ်သာ သဘောထားသည်။ ဒါပေ မယ့် လက်တွေ့မှာတော့ ကိုယ်ရေးကိုယ်တာလုံခြုံမှုဟာ ဆက်နွယ်မှုရှိပါတယ်။ လူတွေ၊ စနစ်တွေနဲ့ အာဏာတွေ ကြားက နေရာလေးမှာ တည်ရှိနေတာပါ။ သင်က တစ်စုံတစ်ယောက်ရဲ့ အဆက်အသွယ်အချက်အလက်တွေ၊ လျှို့ဝှက်ဆက်သွယ်ပြောဆိုထားတဲ့မှတ်တမ်းတွေ ဒါမှမဟုတ် သက်သေခံအချက်အလက်ဖော်ထုတ်တိုင်ကြား လိုသူ သူတစ်ယောက်ရဲ့ သတင်းအချက်အလက်ကို ကိုင်ထားမိတဲ့အချိန်မှာ သင်ချမှတ်လိုက်တဲ့ ဆုံးဖြတ်ချက် တွေဟာ သင့်ရဲ့လုံခြုံရေးကို ပုံဖော်နေသလိုပဲ သူတို့ရဲ့လုံခြုံရေးကိုလည်း ပုံဖော်နေပါတယ်။ ဒီလိုအပြန်အလှန် ဆက်စပ်မှုက ဒစ်ဂျစ်တယ်လုံခြုံရေးကိုပုဂ္ဂိုလ်ရေးဆိုင်ရာ နှစ်သက်မှုတစ်ခုအဖြစ် သာမက လူ့အခွင့်အရေး ဆိုင်ရာ တာဝန်တစ်ခုအဖြစ် ပါ ပြောင်းလဲပေးလိုက်ပါတယ်။ ကျွန်တော်တို့ တစ်ယောက်ကိုတစ်ယောက် တာဝန် ယူမှုရှိအောင် လုပ်ဆောင်ရပါမယ်။ ဒါပေမယ့် စာနာစိတ်နဲ့ လုပ်ဆောင်ရမှာပါ။ ဒစ်ဂျစ်တယ် တစ်ကိုယ်ရေ သန့်ရှင်းမှုဟာ အပြစ်ပေးဖို့အတွက် မဟုတ်ဘဲ အချင်းချင်းကို ကူညီပံ့ပိုးပေးဖို့ ဖြစ်သင့်ပါတယ်။ တစ်စုံတစ်ယောက်က ဖိုင်တစ်ခုကို ကုဒ်ဝှက်ဖို့ မေ့သွားတာ ဒါမှမဟုတ် သူတို့ရဲ့စက်ပစ္စည်းကို လုံခြုံအောင်ထား ဖို့ မေ့သွားတဲ့အခါ အဲဒါကို အရှက်ရစေတာ ဒါမှမဟုတ် အပြစ်ပေးတာမျိုး မလုပ်ဘဲ သင်ကြားပေးဖို့ အခွင့်အရေးတစ်ခုအဖြစ် အသုံးပြုသင့်ပါတယ်။

DigitalHygiene.net က "မကောင်းသောရည်ရွယ်ချက်ရှိသူတစ်ဦးအတွက် အချက်အလက်တိုင်းသည် အရေးကြီးပြီး ပိုမိုများပြားသော အချက်အလက်များကို ရယူဖို့အတွက် လှေကားထစ်တစ်ခုအဖြစ် အသုံးပြု သွားနိုင်ပါသည်" ဟု ဖော်ပြထားပါသည်[77]။ ဤအချက်သည် စောင့်ကြည့်ရန်၊ ဂုဏ်သိက္ခာကျဆင်းအောင် ပြုလုပ်ရန်နှင့် အတိုက်အခံများကို ဖျက်ဆီးရန်အတွက် ရည်ရွယ်ဖန်တီးထားသည့် အစိုးရ သို့မဟုတ် ကော်ပိုရိတ် အဖွဲ့အစည်းများအောက်တွင် တတ်ကြွလုပ်ဆောင်နေသော လှုပ်ရှားတက်ကြွသူများ၊ စည်းရုံးလှုံဆော်သူများနှင့် လူ့အခွင့်အရေးကာကွယ်သူများ အတွက် အထူးမှန်ကန်ပါသည်။ တက်ကြွလှုပ်ရှားသူများ အသုံးပြုရမည့် နည်းဗျူဟာများတွင် နည်းပညာပိုင်းဆိုင်ရာ ကျွမ်းကျင်မှုများ လိုအပ်သည့် နည်းလမ်းများ (IP လိပ်စာ ဖုံးကွယ် ခြင်း သို့မဟုတ် ကိုယ်ပိုင်ကွန်ယက်အတု (VPN) အသုံးပြုခြင်း) မှသည် Google Search သို့မဟုတ် Safari

[77] "What is digital hygiene?" DigitalHygiene.net, accessed May 10, 2025, https://digitalhygiene.net/

ကဲ့သို့သော စောင့်ကြည့်မှုအခြေခံ အမြတ်ထုတ်သည့် ကိရိယာများကို ရှောင်ရှားပြီး ကိုယ်ရေးကိုယ်တာလုံခြုံမှုကို အလေးထားသည့် ကိရိယာများကို (ယခင်အပိုင်းတွင် ကျွန်ုပ်တို့ ဖော်ပြထားသည့်စာရင်းအတိုင်း) အသုံးပြုခြင်းကဲ့သို့သော အလေ့အထများအထိ ပါဝင်ပါသည်။

ဒီလမ်းညွှန်ရဲ့ အများစုကတော့ လက်တွေ့ကျသော ကိရိယာတွေန ့ကျင့်သုံးမှုများအကြောင်း ဖော်ပြထားသော်လည်း၊ ဤလမ်းညွှန်၏ အတိုင်းအတာထက် ကျော်လွန်သည့် ပြဿနာများကို ဖြေရှင်းပေးသည့် အရင်းအမြစ်များကို မီးမောင်းထိုးပြရန်လည်း အရေးကြီးပါသည်။ Cyberwomen လိုမျိုး အဖွဲ့အစည်းတွေဟာ အမျိုးသမီး လူ့အခွင့်အရေး ကာကွယ်စောင့်ရှောက်သူတွေ၊ တက်ကြွလှုပ်ရှားသူတွေန ့ သတင်းထောက်တွေအတွက် အထူးရည်ရွယ်ပြီး ဒစ်ဂျစ်တယ်လုံခြုံရေး သင်ရိုးညွှန်းတမ်းကို ပြုစုပေးထားပါတယ်[78]။ ဒီသင်ရိုးဟာ အမျိုးသမီးတွေကြုံတွေ့ရတဲ့ လက်တွေ့ဘဝ ဒစ်ဂျစ်တယ်တိုက်ခိုက်မှုတွေအပေါ် အခြေခံတဲ့ ဖီမေးနစ် ချဉ်းကပ်မှုကို အလေးထားပါတယ်။ နောက်ထပ် အရင်းအမြစ်များစွာ ပါဝင်တဲ့ ပလက်ဖောင်းတစ်ခုကတော့ digisec.wiki ဖြစ်ပါတယ်။ Cyberwomen နဲ့မတူတဲ့ digisec.wiki ဟာ ကန့်သတ်ချက်တွေကို ကျော်လွှားခြင်း (circumvention) နဲ့ အမည်မဖော်လိုခြင်း (anonymity) တို့ကိုအာရုံစိုက်သည့် ကိရိယာတွေနဲ့ အချက်အလက်တွေ ပါဝင်သည့် အစုအဖွဲ့ အင်တာနက်စာမျက်နှာ (community wiki) တစ်ခုဖြစ်ပါတယ်[79]။ digisec.wiki အင်တာနက်စာမျက်နှာကို အင်္ဂလိပ်၊ ဖိလစ်ပိုင်၊ ထိုင်း၊ မြန်မာ၊ အင်ဒိုနီးရှားနဲ့ ခမာ စတဲ့ ဘာသာစကား ၆ မျိုးနဲ့ ဖော်ပြထားပါတယ်။

Totem သည်လည်း တက်ကြွလှုပ်ရှားသူများနှင့် သတင်းထောက်များအတွက် အထူးထုတ်လုပ်ထားသည့် အင်တာနက်တွင် လေ့လာသင်ယူနိုင်တဲ့ စင်တာတစ်ခု ဖြစ်သည်။ ၎င်းသည် အင်တာနက်ကွန်ယက်လှည့်စား (phishing) တိုက်ခိုက်မှုများမှ ကာကွယ်ခြင်း၊ စက်ပစ္စည်းများ လုံခြုံစေခြင်းနှင့် အင်တာနက်တွင် မည်သူမည်ဝါဖြစ်ကြောင်း ဖော်ထုတ်နိုင်သည့် ကိုယ်ပိုင်အချက်အလက်တွေကို ကာကွယ်ခြင်းကဲ့သို့သော အကြောင်းအရာများအတွက် ကိုယ်ရေးကိုယ်တာလုံခြုံမှုကို လေးစားသော သင်တန်းများကို အခမဲ့နှင့် သင်ပေးပါတယ်[80]။ နောက်ဆုံးအနေဖြင့် Security in a Box သည် တက်ကြွလှုပ်ရှားသူများအသိုင်းအဝိုင်းတွင် ယုံကြည်စိတ်ချရဆုံးနှင့် အကျယ်ပြန့်ဆုံး အသုံးပြုနေသော ဒစ်ဂျစ်တယ်လုံခြုံရေးကိရိယာအစုံတစ်ခုအဖြစ် တည်ရှိနေဆဲဖြစ်သည်[81]။ ၎င်းသည် ဆက်သွယ်ရေး၊ စက်ပစ္စည်းများနှင့် အရေးကြီးသောဖိုင်များကို လုံခြုံအောင်ထားရန်အတွက် ပြည့်စုံသော လမ်းညွှန်များကို ပေးသည်။ ၎င်းကို ထူးခြားစေသောအရာမှာ သင်ကြားမည့်အကြောင်းအရာများကို အမျိုးမျိုးသော အန္တရာယ်ရှိသည့် ပတ်ဝန်းကျင်များ အတွက် အံဝင်ခွင်ကျဖြစ်အောင် ဖန်တီးထားခြင်းဖြစ်သည်။

78 Cyberwomen, *Holistic digital security training curriculum for women human rights defenders (Cyberwomen, 2019)*, https://cyber-women.com/intro/intro.pdf

79 "Main Page" Digisec.wiki, accessed June 15, 2025, https://en.digisec.wiki/wiki/Main_Page

80 "What is Totem?" Totem, accessed May 10, 2025, https://totem-project.org/

81 "What do you need to protect?", Security in a box, accessed June 16, 2025, https://securityinabox.org/en/

ကျွန်ုပ်တို့ ဖော်ပြခဲ့သည့် ဥပမာများအားလုံးသည် ဒစ်ဂျစ်တယ် တစ်ကိုယ်ရေသန့်ရှင်းမှုအကြောင်း တက်ကြွစွာ လေ့လာသင်ယူရမည့် နမူနာပုံစံများ ဖြစ်သည်။ အဘယ်ကြောင့်ဆိုသော် အဆုံးတွင် ဒစ်ဂျစ်တယ် တစ်ကိုယ်ရေသန့်ရှင်းမှုသည် စောင့်ရှောက်မှုပုံစံတစ်မျိုးဖြစ်သောကြောင့် ဖြစ်သည်။ ၎င်းသည် ကျွန်ုပ်တို့၏ တစ်ဦးချင်းဝါဒကို ကျော်လွန်သည့် စောင့်ရှောက်မှုပုံစံတစ်မျိုး ဖြစ်ပြီး၊ အဘယ်ကြောင့်ဆိုသော် ၎င်းတွင် လူမှုအသိုင်းအဝိုင်းနှင့် သင်ပါဝင်သည့် လှုပ်ရှားမှုများလည်း ပါဝင်နေသောကြောင့် ဖြစ်သည်။ ကျွန်ုပ်တို့က ို အတ္တကြီးဖို့၊ ကိုယ်ရေးကိုယ်တာလုံခြုံရေးကို ကိုယ်ပိုင်ပစ္စည်း သို့မဟုတ် ဝယ်ယူရွေးချယ်မှုတစ်ခုအဖြစ် သဘောထားဖို့ အမြဲတစေ တွန်းအားပေးနေသည့် ကမ္ဘာကြီးတွင် စုပေါင်းဒစ်ဂျစ်တယ် တစ်ကိုယ်ရေသန့်ရှင်းမှုကို လိုက်နာကျင့်သုံးခြင်းသည် ထိုအတွေးအခေါ်ကို ပြတ်ပြတ်သားသား ငြင်းပယ်ခြင်းပင် ဖြစ်သည်။ ကျွန်ုပ်တို့သည် မိမိကိုယ်ကို ကာကွယ်ရန် အတွက်သာ ကာကွယ်နေခြင်း မဟုတ်ပါ။ ၎င်းသည် နေ့စဉ်အလေ့အထများ၊ အပြန်အလှန် ပံ့ပိုးကူညီမှုနှင့် တာဝန်ယူမှု များ ကို မျှဝေခြင်းတို့ဖြင့် ဖော်ပြသော စည်းလုံးညီညွတ်မှု တစ်ရပ် ဖြစ်သည်။ အဘယ်ကြောင့်ဆိုသော် အမြတ်ထုတ်ခြင်း အတွက် ပုံဖော်ထားပြီး ၊ ဆန့်ကျင်ကန့်ကွက်ခြင်းကို ရာဇဝတ်မှုအဖြစ် သတ်မှတ်ထားသော စောင့်ကြည့်မှုစီးပွားရေး စနစ်တွင် လုံခြုံရေးဆိုသည်မှာ ကျွန်ုပ်တို့ အတူတကွ တည်ဆောက်ပြီး ကာကွယ်ရမည့် အရာ ဖြစ်သောကြောင့်ပင် ဖြစ်ပါသည်။

စိတ်ကျန်းမာရေး

အလုပ်သမား အခွင့်အရေး၊ အမျိုးသမီးလွတ်မြောက်ရေး၊ LGBTQ+ ဂုဏ်သိက္ခာ၊ သဘာဝပတ်ဝန်းကျင် တရားမျှတမှု သို့မဟုတ် ဒစ်ဂျစ်တယ်လွတ်လပ်ခွင့်တို့ကို ကာကွယ်ခြင်းအပါအဝင် အာဏာကို စိန်ခေါ်တော်လှန်သော တက်ကြွလှုပ်ရှားသူများသည် အမြတ်ထုတ်မှုနှင့် ထိန်းချုပ်မှုများအပေါ်တွင် တည်ဆောက်ထားသော စနစ်များကို တိုက်ရိုက်ဆန့်ကျင်ကြသည်။ ဤအကြောင်းကြောင့် ၎င်းတို့သည် အကြမ်းဖက်မှုနှင့် မကြာခဏ ရင်ဆိုင်ကြုံတွေ့ရသည်။ ဤအကြမ်းဖက်မှုသည် ရုပ်ပိုင်းဆိုင်ရာအရသာမကဘဲ စိတ်ပိုင်းဆိုင်ရာအရပါ ဖြစ်နိုင်ပါသည်။ စွန့်စားရမှု၊ အနှောင့်အယှက်ပေးခံရမှုနှင့် စိတ်ဒဏ်ရာတို့နှင့် အဆက်မပြတ် ထိတွေ့နေရခြင်းသည် စိတ်ဓာတ်ကို ပြိုလဲမှုဖြစ်ပေါ်စေပြီး၊ ၎င်းအခြေအနေမှ အဆက်ဖြတ်ကင်းကွာခြင်းနှင့် ကြောက်ရွံ့မှုကို ဖြစ်ပေါ်စေသည်။ ၎င်းတို့၏ လက်ရှိပတ်ဝန်းကျင်သည် ရန်လိုမှုနည်းပြီး ပိုမိုလက်ခံနိုင်ဖွယ်ရှိသည့် ဘေးကင်းသည်ဟု ထင်ရသော အခြေအနေများတွင်ပင် လူ့အခွင့်အရေး တက်ကြွလှုပ်ရှားသူများသည် ပြင်းထန်သော ပင်ပန်းနွမ်းနယ်မှုနှင့် ကိုယ်စားခံစားရသော စိတ်ဒဏ်ရာ (vicarious trauma) တို့ကို ကြုံတွေ့နေရဆဲဖြစ်သည်။ အကြောင်းမှာ အရင်းရှင် စနစ်က အတိုက်အခံတွေကို ဒီလိုနည်းလမ်းနဲ့ပဲ` စည်းကမ်းထိန်းသိမ်းကြပ်မတ်သောကြောင့်ဖြစ်သည်။ ထို့ကြောင့် ယခုအခါတွင် ဤအပျက်သဘောဆောင်သည့် အကျိုးသက်ရောက်မှုများကို တွန်းလှန်ရန်အတွက် နည်းလမ်းများနှင့် ကိရိယာများရှိရန် ယခင်ကထက် ပိုမိုအရေးကြီးလာပါသည်။

ဤပင်ပန်းနွမ်းနယ်မှုကို တုံ့ပြန်သည့်အနေဖြင့် တက်ကြွလှုပ်ရှားသူများအတွက် အထောက်အကူဖြစ်စေမည့် အခြေခံ အဆောက်အအုံများ ပိုမိုပေါ်ပေါက်လာသည်။ အထူးသဖြင့် တန်ဖိုးရှိသော အရင်းအမြစ်တစ်ခုမှာ

Tactical Technology Collective က Center for Victims of Torture နှင့် Front Line Defenders တို့နှင့် ပူးပေါင်း၍ ရေးဆွဲထား သည့် “အလုံးစုံလုံခြုံရေး- နည်းဗျူဟာကျ လူအခွင့်အရေးခုံခံကာကွယ်သူ လက်စွဲ (Holistic Security: A Strategy Manual for Human Rights Defenders) ဖြစ်ပါသည်။ ၎င်းတို့၏အဆိုအရ မိမိကိုယ်ကို ဂရုစိုက်ခြင်းသည် နိုင်ငံရေးလုပ်ရပ်တစ်ခုဖြစ်ပြီး ၎င်းသည် အတ္တဆန်ခြင်း (selfishness) မဟုတ်ဘဲ မိမိကိုယ်ကို ထိန်းသိမ်းကာကွယ်ခြင်း၏ ဖျက်လိုဖျက်ဆီးသဘောဆောင်သော (subversive) နှင့် နိုင်ငံရေးလုပ်ရပ် (political act) ဖြစ်သည်[82]။ ၎င်းတို့က လုံခြုံရေးကို 'ရုပ်ပိုင်းဆိုင်ရာ အကြမ်းဖက်မှုသာမကဘဲ ဖွဲ့စည်းတည်ဆောက်ပုံဆိုင်ရာ (Structural) ၊ စီးပွားရေး၊ ကျား-မ ပေါ်အခြေခံသော၊ အဖွဲ့အစည်းဆိုင်ရာ အကြမ်းဖက်မှု၊ အနှောင့်အယှက်ပေးမှုနှင့် ဖယ်ကြဉ်ခြင်း' အဖြစ်ပါ ရှုမြင်ရန် ဖော်ပြပေးထားသည်။ ဤအရာများကို နိုင်ငံတွေကသာမက ပုဂ္ဂလိကကော်ပိုရေးရှင်းများ၊ နိုင်ငံတ မဟုတ်သော လက်နက်ကိုင်အဖွဲ့အစည်းများ သို့မဟုတ် ကျွန်ုပ်တို့၏ ကိုယ်ပိုင်အသိုင်းအဝိုင်းများနှင့် ကျွန်ုပ်တို့နှင့် နီးစပ်သူများကပင် ကျူးလွန်နိုင်သည်[83]။ ထို လက်စွဲစာအုပ်တွင် ကာကွယ်သူများအနေဖြင့် ၎င်းတို့၏ မဟာမိတ်များ၊ ရန်သူများနှင့် ကြားနေအဖွဲ့အစည်းများကို ပုံဖော်နိုင်ရန်၊ လုံခြုံရေးသည် ၎င်းတို့အတွက် ဘာကိုဆိုလိုကြောင်း နားလည်နိုင်ရန်နှင့် ဖြစ်နိုင်ခြေရှိသော ဆက်စပ်မဟာဗျူဟာများ၊ အစီအစဉ်များနှင့် နည်းဗျူဟာများကို ရှာဖွေလေ့လာနိုင်ရန်၊ လုံခြုံအောင်ထိန်းသိမ်းဖို့ မူဝါဒများဖန်တီးနိုင်ရန်အတွက် ၎င်းတို့စီမံခန့်ခွဲသည့် အရေးကြီးဆုံးအချက်အလက်များကို မှတ်တမ်းတင်နိုင်ရန် လက်တွေ့ကျသည့် လေ့ကျင့်ခန်းများ ထည့်သွင်းပေးထားသည်[84]။

ဤအသိအမှတ်ပြုမှုကို စိတ်ကျန်းမာရေးပညာရှင်များကလည်း ထပ်လောင်းပြောကြားထားပါသည်။ ကနေဒါ စိတ် ကျန်းမာရေးအသင်း (Canadian Mental Health Association) က ကိုယ်အားစိတ်အား ချုံးချုံးကျခြင်းကို 'ရုပ်ပိုင်းဆိုင်ရာနှင့် စိတ်ပိုင်းဆိုင်ရာ ပင်ပန်းနွမ်းနယ်မှုကို မကြာခဏဖြစ်စေသည့် စဉ်ဆက်မပြတ် ဖိစီးမှုအခြေအနေ' အဖြစ် သတ်မှတ်ခဲ့ပြီး ကိုယ်စားခံစားရသော ထိခိုက်စိတ်ဒဏ်ရာများ (vicarious trauma) သည် ဒေါသထွက်ခြင်း၊ အပြစ်ရှိသည်ဟု ခံစားရခြင်း၊ မျှော်လင့်ချက်မဲ့ခြင်းနှင့် မောပန်းနွမ်းနယ်ခြင်းတို့ကဲ့သို့ ပြင်းထန်သော စိတ်ပိုင်းဆိုင်ရာ ထိခိုက်မှုများကို ဖြစ်ပေါ်စေသည်[85]။ ဤလမ်းညွှန်ချက်သည် အထောက်အကူပြုကွန်ရက်များ တည်ဆောက်ခြင်း၊ တက်ကြွလှုပ်ရှားမှု လုပ်ငန်း ပြင်ပတွင်လည်း အချိန်ပေးခြင်း၊ တရားထိုင်ခြင်း၊ အောင်မြင်မှုများကို ဂုဏ်ပြုအောင်ပွဲခံ ခြင်း၊ ကျေးဇူးတင်စရာများကို မှတ်မိစေရန် သို့မဟုတ် အရေးတယူဆောက်ရွက်ရန်အတွက် စိတ်ဒဏ်ရာများကို မှတ်သားထားရန် မှတ်တမ်းရေးသားပြီ၊ လူမှုကွန်ယက်မီဒီယာနှင့် နည်းပညာအပေါ် အချိန်အကန့်အသတ်ထားရှိခြင်း သို့မဟုတ် အသိပေးချက်များကို ပိတ်ထားခြင်းကဲ့သို့သော နယ်နိမိတ်များကို သတ်မှတ်ခြင်းဖြင့် စွမ်းဆောင်ရည်နှင့် ကိုယ်ပိုင်ဆုံးဖြတ်နိုင်စွမ်းကို ပြန်လည်ရရှိစေရန် ရည်ရွယ်သည်။

---

82 Tactical Technology Collective, Holistic Security A Strategy Manual for Human Rights Defenders (Tactical Technology Collective, 2016), 21, https://holistic-security.tacticaltech.org/ckeditor_assets/attachments/61/hs_complete_hires.pdf

83 Tactical Technology Collective, 12

84 Tactical Technology Collective, 56

85 “Mental Health And Self-Care For Activists”, Canadian Mental Health Association, accessed May 17, 2025, https://cmha-yr.on.ca/mental-health-and-self-care-for-activists/

အပြည်ပြည်ဆိုင်ရာလွတ်ငြိမ်းချမ်းသာခွင့် အဖွဲ့ (Amnesty International) ကလည်း X (ယခင် Twitter)၊ Facebook နှင့် YouTube တို့တွင် စိတ်ဒဏ်ရာဖြစ်စေနိုင်သော အကြောင်းအရာများကို ကိုင်တွယ်ဖြေရှင်းရန် လက်တွေ့ကျသော အကြံဉာဏ်များ ပေးထားသည်[86]။ ဥပမာအားဖြင့်၊ လူမှုကွန်ယက်မီဒီယာများတွင် ဗီဒီယိုများ အလိုအလျောက်ဖွင့်ခြင်းကို ပိတ်ထားရန်၊ မလိုအပ်သည့်အခါ အသံကို ပိတ်ထားရန်နှင့် စာပို့ဆက်သွယ်သည့် ပလက်ဖောင်းများတွင် အလိုအလျောက် ဒေါင်းလုဒ်လုပ်ခြင်းကို တားဆီးရန်တို့ ဖြစ်သည်။ ၎င်းတို့သည် ဒစ်ဂျစ်တယ် စိတ်ဒဏ်ရာနှင့် ထိတွေ့ ခြင်းအပေါ် ထိန်းချုပ်မှုကို ပြန်လည်ရယူရန်အတွက် သေးငယ်သော်လည်း အစွမ်းထက်သည့် နည်းလမ်းများဖြစ်သည်။ အဘယ်ကြောင့်ဆိုသော် မိမိကိုယ်ကို ထိန်းသိမ်းခြင်းသည် ဆုတ်ခွာခြင်းမဟုတ်ပါ။ ၎င်းသည် ရုန်းကန်လှုပ်ရှားမှုကို အလားအလားဖြစ်နိုင်အောင် လုပ်ပေးသည်။ The Commons အတွက် စာရေးရာတွင် Helen Cox က တက်ကြွလှုပ်ရှား သူများအနေဖြင့် မိမိကိုယ်ကို ရေရှည်တည်တံ့အောင် မည်သို့လုပ်ဆောင်ကြသနည်းဟူသော မေးခွန်းအတွက် လူ ၂၀၀ နီးပါးထံမှ အဖြေများကို ပေါင်းစည်းခဲ့သည်။ အချို့က စွမ်းအင်နှင့် အာရုံစူးစိုက်မှုကို ထိန်းသိမ်းရန် စည်းရုံးရေးလှုပ်ရှားမှုများနှင့် အဖွဲ့များတွင် ပါဝင်ခြင်းကို ကန့်သတ်ဖို့ ငြင်းဆိုရန် လိုအပ်ကြောင်း ပြောဆိုခဲ့ကြသည်။ အခြားသူများကတော့ ကောင်းမွန်စွာ အိပ်စက်ခြင်း၊ သင့်လျော်သောအာဟာရနှင့် ပုံမှန်ကိုယ်လက်လှုပ်ရှားမှုကဲ့သို့ မကြာခဏ လျစ်လျူရှုခံရသည့် အခြေခံအချက်များကို ထောက်ပြခဲ့ကြသည်။ များစွာသောသူတို့သည် သဘာဝတရား၏ အားသစ်လောင်းပေးနိုင်သော စွမ်းအား၊ အချိန်နှင့် ပတ်သက်၍ နယ်နိမိတ်များ သတ်မှတ်ခြင်း၏အရေးပါမှုနှင့် အနားယူချိန်များ သတ်မှတ်ခြင်း၏ စည်းကမ်းကို အလေးပေးပြောကြားခဲ့သည်။ သို့သော် နောက်ဆုံးတွင် ထိုအဖြေများက ကျွန်ုပ်တို့ကို သတိပေးသည်မှာ တတ်ကြွ လှုပ်ရှားမှုလုပ်ငန်းတွင် ရေရှည်တည်တံ့စေရန် တစ်ခုတည်းသောနည်းလမ်းမရှိပေ။ ကျွန်ုပ်တို့သည် အကြောင်းတရားတစ်ခုအတွက်သာမက မိမိတို့အတွက်နှင့် အချင်းချင်းအတွက်ပါ တိုက်ပွဲဝင်နေခြင်းဖြစ်သည်။

ဗဟုသုတမျှဝေခြင်း (Knowledge-sharing)

လူ့အခွင့်အရေးအတွက် ကမ္ဘာလုံးဆိုင်ရာ ရုန်းကန်လှုပ်ရှားမှုသည် အသိပညာ၊ ကိရိယာများနှင့် နည်းဗျူဟာများကို စုပေါင်းမျှဝေနိုင်စွမ်းအပေါ် မူတည်သည်။ နယ်နိမိတ်များ၊ လှုပ်ရှားမှုများနှင့် အရေးများ တစ်လျှောက်တွင် တက်ကြွလှုပ်ရှားသူများသည် အရင်းအမြစ်များ စုပေါင်းခြင်း၊ စည်းလုံးညီညွတ်မှု တည်ဆောက်ခြင်းနှင့် ဖိနှိပ်မှုကို တွန်းလှန်နိုင်စွမ်းကို မြှင့်တင်ခြင်းဖြင့် တစ်ဦးနှင့်တစ်ဦး အပြန်အလှန် သင်ယူနိုင်သည်။ အသိပညာများ ပျံ့နှံ့သောအခါ အာဏာ/တတ်နိုင်စွမ်း (ကိုယ်စွမ်း ညက်စွမ်း) လည်း ပျံ့နှံ့သည်။

လူ့အခွင့်အရေးကာကွယ်သူများ၏ လက်တွေ့ဘဝများကို မီးမောင်းထိုး ထင်ရှားစေသည့် လှုပ်ရှားမှုများသည် အသိပညာပေးခြင်းထက် ပိုမိုလုပ်ဆောင်နိုင်စွမ်းရှိသည်။ ၎င်းတို့သည် အာဏာရှင်စနစ်က လိုလားအားကိုးသော

[86] "The hidden victims of repression – how activists and reporters can protect themselves from secondary trauma," Amnesty International, published February 20, 2019, https://www.amnesty.org/en/latest/news/2019/02/how-activists-and-reporters-can-protect-themselves-from-secondary-trauma/

တိတ်တိတ်နေမှုကို ဖြိုခွဲပြီး အနိုင်ကျင့်မှုများကို တိုက်ဖျက်ရန် နိုင်ငံတကာဖိအားကို တည်ဆောက်ရယူသည်။ Front Line Defenders (FLD) ကဲ့သို့သော အဖွဲ့အစည်းများသည် ဤပုံပိုးကူညီမှုကို ပိုမိုခိုင်မာစေရန် တည်ရှိနေခြင်းဖြစ်သည်[87]။ FLD တွင် လူ့အခွင့်အရေး ကာကွယ်သူများအတွက် ဖြစ်လာနိုင်သည့် အန္တရာယ်ကိုခွဲခြမ်းစိတ်ဖြာခြင်းနှင့် ကာကွယ်ရေးစီမံကိန်းရေးဆွဲခြင်း၊ အနားယူအပန်းဖြေခြင်း၊ ကာကွယ်စောင့်ရှောက်ရေး ထောက်ပံ့ကြေးများအပြင် အရေးပေါ်ဖုန်းခေါ်ဆိုမှုနံပါတ်ကဲ့သို့သော ကိရိယာများစွာရှိပြီး၊ ၎င်းသည် 'လူ့အခွင့်အရေး ကာကွယ်သူများကို အာရဗီ၊ အင်္ဂလိပ်၊ ပြင်သစ်၊ ရုရှား သို့မဟုတ် စပိန်ဘာသာစကားပြောသူတစ်ဦးထံသို့ လွှဲပြောင်းပေးပြီး အရေးပေါ် အခြေအနေ တွင် မည်သို့အကောင်းဆုံး ပံ့ပိုးကူညီရမည်ကို ဆုံးဖြတ်ရာတွင် အကူအညီပေးမည်' ဖြစ်သည်[88]။

တစ်ချိန်တည်းမှာပင်၊ ဒစ်ဂျစ်တယ်ကမ္ဘာသည် တက်ကြွလှုပ်ရှားသူများကို ကိရိယာများဆင်ပေးရန်အတွက် လမ်းကြောင်းသစ်များ ဖွင့်ပေးခဲ့သည်။ FreedomLab ၏ Starlight Stadium ကဲ့သို့သော ဒစ်ဂျစ်တယ် ပလက်ဖောင်းများသည် လူ့အခွင့်အရေးစောင့်ကြည့်လေ့လာခြင်းဆိုင်ရာ ကျွမ်းကျင်မှုများကို ဒီမိုကရေစီနည်းကျ လက်လှမ်းမီစေသည်[89]။ Starlight Stadium သည် အပြန်အလှန်တုံ့ပြန်ဆွေးနွေးနိုင်သော ပညာရေးဆိုင်ရာ ကိရိယာတစ်ခုဖြစ်ပြီး ကနဦး ပြဿနာအကဲဖြတ်ခြင်းနှင့် သတင်းအချက်အလက်စုဆောင်းခြင်းမှစ၍ ခွဲခြမ်းစိတ်ဖြာခြင်း၊ အစီရင်ခံခြင်းနှင့် စည်းရုံးလှုံ့ဆော်ခြင်း အထိ လူ့အခွင့်အရေးလှုပ်ရှားမှုလုပ်ငန်းစဉ် အစမှအဆုံး တစ်ခုလုံးကို အသုံးပြုသူများအား ဖြတ်သန်းလေ့လာစေပါသည်။ ၎င်းသည် ကာကွယ်သူများအား လုပ်ကိုင်ဆောင် ရွက်နိုင်ရန်အတွက် ယုံကြည်မှုနှင့် စွမ်းဆောင်ရည်နှစ်ရပ်စလုံးကို တပ်ဆင်ပေးရန် ရည်ရွယ်သည့် လက်လှမ်းမီနိုင်သော၊ တတ်ကြွလှုပ်ရှားမှုအသားပေး သင်ယူမှုအခြေခံ အဆောက်အအုံ ၏ လှိုင်းသစ်တစ်ခုကို ကိုယ်စားပြုပါသည်။ လက်တွေ့ကျသော စွမ်းဆောင်ရည်တည်ဆောက်မှုအပေါ် အလေးပေးမှုကို Amnesty International ၏ Security Lab ကလည်း မျှဝေထားသည်။ ၎င်းသည် Access Now, Front Line Defenders, Human Rights Watch, InterSecLab, SocialTic နှင့် Reporters sans Frontières (RSF) စသည့် အဖွဲ့အစည်းများနှင့် မိတ်ဖက်အဖွဲ့အစည်းကို ပူးပေါင်းဆောင်ရွက်မှု အဖြစ် စတင်ခဲ့ပါသည်[90]။ ၎င်းတို့သည် အတူတကွ ခြိမ်းခြောက်မှုဆိုင်ရာ အချက်အလက်များကို မျှဝေခြင်း၊ လွတ်လပ်သော အမှုအခင်းစစ်ဆေးခြင်းနှင့် စုပေါင်းဒစ်ဂျစ်တယ် တရားဝင်သက်သေခံ အထောက်အထား ဆိုင်ရာ သုတေသနပြုခြင်းတို့မှတစ်ဆင့် ဒစ်ဂျစ်တယ်အခွင့်အရေးများကို ကာကွယ်ရန် ခိုင်မာသော ဂေဟစနစ်ကို ဖန်တီး နေကြသည်။ ဤကြိုးပမ်းမှု၏ အဓိကအချက်သော့ချက်မှာ ကမ္ဘာတစ်ဝန်းမှ အရပ်ဘက်လူ့အဖွဲ့အစည်းဆိုင်ရာ နည်းပညာရှင်များကို စုစည်းထားသည့် Digital Forensic Fellowship အစီအစဉ်ဖြစ်သည်။ Fellowship အဖွဲ့ဝင်များသည်

[87] "About Us", Frontline Defenders, accessed May 17, 2025, https://www.frontlinedefenders.org/en/who-we-are
[88] "Emergency Contact for Human Rights Defenders", Front Line Defenders, accessed May 23, 2025, https://www.frontlinedefenders.org/en/emergency-contact-human-rights-defenders
[89] "Starlight Stadium", FreedomLab, accessed May 16, 2025, https://freedomlab.io/starlight-stadium/
[90] "Partners and Support", Amnesty International, accessed May 13, 2025, https://securitylab.amnesty.org/partners-and-support/

၎င်းတို့၏ ဒစ်ဂျစ်တယ် တရားဝင်သက်သေခံအထောက်အထားဆိုင်ရာ ကျွမ်းကျင်မှုကို နက်ရှိုင်းစေရန် အတွေ့အကြုံရှိ စုံစမ်းစစ်ဆေးသူများနှင့် အနီးကပ်လက်တွဲလုပ်ဆောင်ကြသည်။

ဤအခြေခံအဆောက်အအုံများသည် ဇာတ်ကြောင်းများကို ပုံဖော်ပြောင်းလဲခဲ့ပြီး တာဝန်ယူမှု၊ တာဝန်ခံမှုကို ဖိအားပေးဖြစ်ပေါ်စေခဲ့သော လှုပ်ရှားမှုများအဖြစ် မကြာခဏဆိုသလို အသွင်ပြောင်းသည်။ ထိရောက်သော ဥပမာတစ်ခုမှာ အီရန်နိုင်ငံအတွင်း Signal ပလက်ဖောင်းကို ပိတ်ဆို့မှုအတွက် တုံ့ပြန်မှုတစ်ခုဖြစ်သော Signal ၏ #IranASignalProxy လှုပ်ရှားမှု ဖြစ်သည်။ ဤပဏာမခြေလှမ်းက Signal အသုံးပြုသူများအား အီရန်နိုင်ငံကလူများကို Signal နှင့် ချိတ်ဆက်နိုင်ရန် ကူညီဖို့ ကိုယ်ပိုင် ကြားခံဆာဗာ (proxy server) များ တည်ထောင်ပေးဖို့ ဖိတ်ခေါ်နိုင်ခဲ့ပါသည်[91]။အလားတူပင်၊ နိုင်ဂျီးရီးယားတွင် Citizens' Gavel သည် တရားမျှတမှုလက်လှမ်းမှီစေရေး ပိုမိုကောင်းမွန်လာစေရန် လုပ်ဆောင်နေသည်။ ၎င်းတို့၏ Podus အပလီကေးရှင်းသည် ရဲတပ်ဖွဲ့တွေရဲ့ အကြမ်းဖက်မှုနှင့် အခြားအခွင့်အရေးချိုးဖောက်မှုများ ခံရသူများကို အခမဲ့ရှေ့နေများနှင့် ချိတ်ဆက်ပေးခြင်းဖြင့် ဥပဒေအကူအညီရယူခြင်း လုပ်ငန်းစဉ်ကို ရိုးရှင်းစေသည်[92]။ တစ်ချိန်တည်းတွင်၊ မြန်မာအင်တာနက်စီမံကိန်း (Myanmar Internet Project) သည် ၂၀၂၅ ခုနှစ် ငလျင်ကဲ့သို့သော လူသားချင်းစာနာထောက်ထားမှုဆိုင်ရာ အကျပ်အတည်းများအတွင်း နိုင်ငံကဦးဆောင်သည့် အင်တာနက်ဖြတ်တောက် မှု၏ ဆိုးရွားလှသော သက်ရောက်မှုများကို ဖော်ထုတ်ရန် လုပ်ဆောင်ခဲ့သည်[93]။

ဥရောပတွင် European Digital Rights (EDRi) ကွန်ရက်မှ ဦးဆောင်သော Reclaim Your Face ကမ်ပိန်းသည် ဇီဝဆိုင်ရာအချက်အလက်တွေကို စောင့်ကြည့်မှုများအပေါ် အလွန်အကျူးပြုလုပ် ခြင်းကို တိုက်ရိုက်ပစ်မှတ်ထား ခဲ့သည်။ ၎င်းတို့သည် မျက်နှာမှတ်သားမှုနည်းပညာကို ကိုယ်ရေးကိုယ်တာလုံခြုံရေးအတွက်သာမကဘဲ အများပြည်သူ၏ စုပေါင်းဘေးကင်းလုံခြုံရေးနှင့် ကိုယ်ပိုင်ဆုံးဖြတ်ပိုင်ခွင့်တို့ အတွက်ပါ ခြိမ်းခြောက်မှုတစ်ခုအဖြစ် ပုံဖော်ခဲ့ကြသည်။ ဤ လှုပ်ရှားမှုသည် အစိုးရများနှင့် ကော်ပိုရေးရှင်းများက လူအများကို အထူးသဖြင့် ပစ်ပယ်ခံထားရသော သို့မဟုတ် လက်ရှိအခြေအနေကို ဆန့်ကျင်နေသူများကို စောင့်ကြည့်ရန်၊ ထိန်းချုပ်ရန်နှင့် စည်းကမ်းသတ်မှတ်ရန်အတွက် အမြတ်ထုတ်သည့် နည်းပညာများကို မည်သို့အသုံးချနေသည်ကို ဖော်ထုတ်ပြသခဲ့သည်[94]။ ဤ စီမံကိန်းနှင့် ကမ်ပိန်းများ အောင်မြင်ခဲ့ခြင်းမှာ လူမှုအသိုင်းအဝိုင်းများက ဝမ်းနည်းပူဆွေးမှုကို သာမကဘဲ` အချက်အလက်များ၊ မဟာဗျူဟာများနှင့် အရေးအကြီးဆုံးမှာ အစသစ်တစ်ခုအတွက်

---

91 meredith-signal (Meredith Whittaker), “Help people in Iran reconnect to Signal – a request to our community”
Signal.org (blog), September 22, 2022, https://signal.org/blog/run-a-proxy/

92 “Access to Justice Empowering Justice, Connecting Lives,” Podus, accessed June 16, 2025, https://podus.org/.

93 “Digital Coup Timeline,”Myanmar Internet Project, accessed June 16, 2025, https://www.myanmarinternet.info/

94 **SHARE Foundation, Hermes Center, Bits of Freedom, ARTICLE19, Homo Digitalis and EDRi,** “Campaign “Reclaim Your Face” calls for a Ban on Biometric Mass Surveillance”, EDRi, November 12, 2020, *https://edri.org/our-work/campaign-reclaim-your-face-calls-for-a-ban-on-biometric-mass-surveillance/*

မျှော်လင့်ချက်၊ တရားမျှတမှုနှင့် တာဝန်ခံမှုတို့အတွက် မျှော်လင့်ချက်များကိုပါ မျှဝေခဲ့ကြသောကြောင့် ဖြစ်သည်။

အရေးပေါ်နှင့် အကူအညီပေးရေး ကွန်ရက်များ

ပူးပေါင်းဆောင်ရွက်မှု ခိုင်မာစေရန်အတွက် အကူအညီပေးရေး ကွန်ရက်တစ်ခုကို တည်ထောင်ခြင်း သို့မဟုတ် ယင်းကွန်ရက်၏ အစိတ်အပိုင်းတစ်ခု ဖြစ်လာခြင်းသည် မရှိမဖြစ်လိုအပ်ပါသည်။ ကွန်ရက်ရှိ စိတ်တူကိုယ်တူနှင့် အချင်းချင်းပံ့ပိုးကူညီသူများသည် ကိုယ်ရေးကိုယ်တာလုံခြုံမှု၊ ဒစ်ဂျစ်တယ်သန့်ရှင်းရေးနှင့် ကိုယ်ခန္ဓာနှင့် စိတ်ကျန်းမာရေးတို့အတွက် အကြံဉာဏ်များ ပေးကြပြီး အရင်းအမြစ်များ၊ အသိပညာနှင့် အတွေ့အကြုံများ (ဥပမာ- ဆေးဘက်ဆိုင်ရာ၊ ဥပဒေရေးရာ သို့မဟုတ် ငွေကြေးအကူအညီနှင့် ကိုယ်ကာယလုံခြုံမှုတို့ကို မည်သို့နှင့် မည်သည့်နေရာတွင် ရှာဖွေရမည် စသည်ဖြင့်) မျှဝေကြသည်။ ယုံကြည်စိတ်ချရသော ဆက်သွယ်ဆောင်ရွက်သူများ ပါဝင်ပြီး၊ လုံခြုံသော ဆက်သွယ်ရေးလမ်းကြောင်းများကို အသုံးပြုကာ ပုံမှန် လုပ်ထုံးလုပ်နည်းများကို လိုက်နာသည့် ကွန်ရက်တစ်ခု ဖြစ်ရန်လည်း အရေးကြီးပါသည်။ အောက်တွင် ဖော်ပြထားသည်မှာ အန္တရာယ်နှင့် ရင်ဆိုင်နေရသော သို့မဟုတ် ဆိုက်ဘာအနှောင့်အယှက် ခံနေရသော တက်ကြွလှုပ်ရှားသူများအတွက် အရေးပေါ်အကူအညီ ပေးသည့် အဖွဲ့အစည်းများ၏ စာရင်းဖြစ်ပြီး ၎င်းသည် ပြည့်စုံသောစာရင်းမဟုတ်ပါ။,

အဖွဲ့အစည်း အမည်	အီးမေး	ဖုန်းနံပါတ်	ဘာသာစကား	တည်နေရာ
Protect Defenders	contact@protectdefenders.eu secure contact form: https://protectdefenders.eu/emergency-contact/	+35312100489	အင်္ဂလိပ်၊ စပိန်၊ ရုရှား၊ အာရဗီ၊ ပြင်သစ်၊ ပေါ်တူဂီ၊ တူရကီ	နေရာအနှံ (Global)
7amleh	help@7amleh.org	+972533302167	အင်္ဂလိပ်၊ အာရဗီ၊	အနောက်အာရှ (အရှေ့အလယ်ပိုင်း)
Access Now	help@accessnow.org		အင်္ဂလိပ်၊ စပိန်၊ ပြင်သစ်၊ ဂျာမန်၊ ပေါ်တူဂီ၊ ဖိလစ်ပိုင်၊ ရုရှား၊ အာရဗီ၊ အီတလီ၊ ယူကရိန်း၊ တာဂျစ်	နေရာအနှံ (Global)
Co-creation hub	digitalsecurity@cchubnigeria.com	+23412950555	အင်္ဂလိပ်	နိုင်ဂျီးရီးယား
Civilsphere Project	civilsphere@aic.fel.cvut.cz		အင်္ဂလိပ်၊ စပိန်	ချက်ကီယာ
COLNODO	info@escueladeseguridaddigital.co	+573156021376	အင်္ဂလိပ်၊ စပိန်	
CIRCLU	info@circl.lu	+352 247 88444	အင်္ဂလိပ်၊ ဂျာမန်၊ ပြင်သစ်၊ လူဇင်ဘတ်	လူဇင်ဘတ်

TibCERT	info@tibcert.org	+919816170738	တိဗက်၊ အင်္ဂလိပ်	အိန္ဒိယ
SHARECERT	emergency@sharecert.rs	+381 64 089 70 67	ဆားဘီးယား၊ မက်ဆီဒိုးနီးယား	
Digital Rights Foundation	helpdesk@digitalrightsfoundation.pk	9280039393	Pakistani, English အူရဒူ၊ အင်္ဂလိပ်	ပါကစ္စတန်
Digital Defense Fund	team@digitaldefensefund.org		အင်္ဂလိပ်၊ စပိန်၊ ဗီယက်နမ်	
Digital Society of Zimbabwe	helpline@digitalsociety.africa	+27762982174	အင်္ဂလိပ်၊ ရှိန်နာ၊ အင်ဒီဘယ်လီ၊ ဇူလူ	ဇင်ဘာဘွေ
Nothing2Hide	help@tech4press.org	+33 7 81 37 80 08	အင်္ဂလိပ်၊ ပြင်သစ်	
Deflect	support@equalit.ie		အင်္ဂလိပ်၊ ပြင်သစ်၊ ရုရှား၊ စပိန်၊ အင်ဒိုနီးရှား၊ ဖိလစ်ပိုင်	

အပိုင်း ၄- အရင်းအမြစ်များ

ဤသည်မှာ ခရီးသွားသည့်အခါ ပုံနှိပ်ပြီး အိတ်ဆောင်ထားနိုင်သည့် အရေးပေါ်အဆက်အသွယ်ပုံစံပုံစံတစ်ခု ဖြစ်သည်။ ၎င်းတွင် ဥပဒေအကူအညီနှင့် အဓိကအရေးပေါ်အဆက်အသွယ်များအပါအဝင် လိုအပ်သော အခြေခံအချက်အလက် အားလုံး ပါဝင်ပါသည်။ အမြဲတမ်း ဆောင်ထားပါ။

သင်၏ ကိုယ်ရေးအချက်အလက်များ

- အမည်- _____
- မွေးသက္ကရာဇ်- _____
- နိုင်ငံသား- _____
- ဓာတ်မတည့်ခြင်း/ကျန်းမာရေးအခြေအနေများ- _____
- သွေးအမျိုးအစား (သိရှိပါက)- _____

အဓိက အရေးပေါ်ဆက်သွယ်ရန်ပုဂ္ဂိုလ်

- အမည်- _____
- တော်စပ်ပုံ- _____
- ဖုန်းနံပါတ် (နိုင်ငံကုဒ်ပါ)- _____
- ဆက်သွယ်စာပို့နိုင်သောအပလီကေးရှင်း-_____
- အီးမေးလ်- _____

ဥပဒေအကူအညီ/ရှေ့နေ အဆက်အသွယ်

- အမည်/အဖွဲ့အစည်း- _____
- ဖုန်းနံပါတ်- _____
- လုံခြုံသော ဆက်သွယ်ရေးနည်းလမ်း- _____
- မှတ်စုများ (အမှုနံပါတ်၊ ပြောဆိုနိုင်သောဘာသာစကားများ စသည်)- _____

အဖွဲ့အစည်း/အဖွဲ့ ဆက်သွယ်ရန်ပုဂ္ဂိုလ်

- အမည်/ရာထူး- _____
- ဖုန်းနံပါတ်- _____
- လုံခြုံသော ဆက်သွယ်ရေးနည်းလမ်း- _____
- အရန်သင့်ဆက်သွယ်ရန်ပုဂ္ဂိုလ် (အဓိကပုဂ္ဂိုလ်ကိုဆက်သွယ်မရပါက) _____

ဆိုက်ဘာလုံခြုံရေး စစ်ဆေးရန်စာရင်း

သင့်အကောင့်များကို လုံခြုံအောင် သေချာထားပါ

- အကောင့်တိုင်းအတွက် ရှည်လျားပြီး ထူးခြားသည့် စကားဝှက်များကို အသုံးပြုပါ။
- ဖြစ်နိုင်သည့်နေရာတိုင်းတွင် အချက်များစွာဖြင့် စစ်မှန်ကြောင်း အတည်ပြုခြင်း MFA (Multi-Factor Authentication) ကို ဖွင့်ထားပါ။
- အကောင့်များအတွက် စကားဝှက်များကို ထပ်ခါတလဲလဲ ပြန်မသုံးပါနှင့်။
- ယုံကြည်စိတ်ချရသော စကားဝှက်မန်နေဂျာ (password manager) ကို အသုံးပြုပါ။

သင့်စက်ပစ္စည်းများကို လုံခြုံအောင်ထားပါ

- သင့်ဖုန်း၊ လက်ပ်တော့နှင့် အပလီကေးရှင်းများကို အချိန်တိုင်း အဆင်မြှင့်တင်မှုလုပ်ထားပါ။
- ကွန်ပြူတာသုံး ဓာတ်ပြား တစ်ခုလုံးကို အလုံးစုံစာဝှက်လျှို့ဝှက်ကုဒ်စနစ် ထားခြင်းကိုအသုံးပြုပါ (full-disk encryption)
- စက်ပစ္စည်းများကို အသုံးမပြုဘဲ ထားပါက အလိုအလျောက်သော့ခတ်ရန် သတ်မှတ်ပါ။

ခရီးသွားသည့်အခါ

- ခရီးမဆိုက်ရောက်မီ နှင့် သင့်အကောင့်များ (အီးမေးလ်၊ ဆက်သွယ်စာပို့နိုင်သောအပလီကေးရှင်းများ၊ cloud သိုလှောင်မှု) အားလုံးမှ ထွက်လိုက်ပါ။
- မျက်နှာကိုအသုံးပြုပြီး လုံခြုံရေးစနစ်ဖွင့်လှစ်မှု ၊ ဇီဝဆိုင်ရာအချက်အလက်တွေ (biometrics) သို့မဟုတ် အသံဖြင့် သော့ဖွင့်ခြင်းတို့ကို ဖယ်ရှားပါ။ ယင်းအစား ခိုင်မာသော PIN နံပါတ် သို့မဟုတ် စကားစုကို အသုံးပြုပါ။
- ခရီးမသွားမီ အရေးကြီးသော အဆက်အသွယ်များ၊ စကားပြောဆိုမှုများနှင့် စာရွက်စာတမ်းများကို ဖျက်ပစ်ပါ (လုံခြုံသော အရန်သိမ်းဆည်းမှုများကို အခြားတစ်နေရာတွင် ထားပါ)။
- ခရီးမသွားမီ အရေးကြီးသည့် အချက်အလက်များကို အိမ်တွင် အရန်သိမ်းဆည်းပါ။
- နယ်စပ်ဖြတ်ကျော်နေစဉ် သင့်ဖုန်းက အချက်အလက်အားလုံး လုံးဝရှင်းလင်းခြင်းမျိုး မလုပ်ပါနှင့်။ ထိုသို့ပြုလုပ်ပါက နယ်စပ်အာဏာပိုင်များက သင့်ကို ပိုမိုစစ်ဆေးရန် သတိပေးသလို ဖြစ်နိုင်ပါသည်။
- အရေးကြီးသည့် ဖိုင်များကို သယ်ဆောင်ရန် လိုအပ်ပါက hardware-encrypted USB drives များကို အသုံးပြုရန် စဉ်းစားပါ။

- သင့်အားသွင်းကြိုး သို့မဟုတ် USB ကေဘယ်ကို သီးသန့်မဟုတ်သော အားသွင်းရန်နေရာများ၊ အားသွင်းစခန်းများ သို့မဟုတ် အများသုံး အားသွင်နေရာများတွင် တပ်ဆင်ခြင်းကို ရှောင်ရှားပါ။ သင့်ကိုယ်ပိုင် ပါဝါဘင်္ကထရီ သို့မဟုတ် ဒေတာပိတ်ဆို့သည့် USB adapter ကို အသုံးပြုပါ။
- ဟိုတယ် Wi-Fi၊ လေဆိပ်အားသွင်းစခန်းများ သို့မဟုတ် မျှဝေအသုံးပြုသော ကွန်ပျူတာများကို အသုံးပြုရာ တွင် သတိထားပါ။
- သင့်စက်ပစ္စည်းကို အသိမ်းခံရပါက သို့မဟုတ် သော့ဖွင့်ရန် အတင်းအကျပ် တောင်းဆိုခံရပါက မည်သို့လုပ် ဆောင်မည်ကို ကြိုတင်စီစဉ်ထားပါ။
- အရေးပေါ်ဆက်သွယ်ရန် အချက်အလက်နှင့် အဓိကအချက်အလက်များကို ဖုန်းထဲတွင်သာမက စာရွက်ပေါ် တွင်ပါ ဆောင်ထားပါ။ (အထက်ပါ ပုံစံကို ကြည့်ပါ)
- ခရီးသွားရင်း ကိုယ်တိုင်ရိုက်ပုံများ (selfies) သို့မဟုတ် လက်ရှိတည်နေရာကို လူမှုကွန်ရက်တွင် တင်ခြင်းမျိုး မလုပ်ပါနှင့်။
- သင့်ကို အန္တရာယ်ဖြစ်စေနိုင်သည့် တက်ကြွလှုပ်ရှားမှုများနှင့် ဆက်စပ်နေသော မလိုအပ်သည့် မှတ်ပုံတင်များ၊ အဖွဲ့ဝင်ကတ်များ သို့မဟုတ် စာရွက်စာတမ်းများကို မသယ်ဆောင်ပါနှင့်။

သင်၏ ဆက်သွယ်မှုပြောဆိုမှုများကို ကာကွယ်ပါ

- စကားပြောဆိုမှုများကို အလုံးစုံအလုံးစုံစာဝှက်လျှို့ဝှက်ကုဒ်စနစ် (end-to-end encrypted) လုပ်ပေးသည့် အပလီကေးရှင်းများကို အသုံးပြုပါ။
- အရေးကြီးသော ဆက်သွယ်မှုများအတွက် ဖုန်းလိုင်းမှစာပို့ခြင်း (SMS) ကို ရှောင်ပါ။
- အရေးကြီးသည့် အချက်အလက်များ မမျှဝေမီ လက်ခံမည့်သူ၏ အချက်အလက်ကို နှစ်ခါပြန်စစ်ဆေးပါ။
- Facebook Messenger သို့မဟုတ် Instagram DMs ကဲ့သို့သော ပလက်ဖောင်းကြီးများကို ကိုယ်ရေးကိုယ်တာအကြောင်း စကားပြောဆိုမှုများအတွက် မယုံကြည်ပါနှင့်။
- ညဏ်ရည်တု (AI) ကိရိယာများကို အသုံးပြုရာတွင် သတိထားပါ။

သင်၏ ကွန်ရက်ကို ကာကွယ်ပါ

- အများသုံး သို့မဟုတ် မျှဝေသုံးသော Wi-Fi တွင် ကိုယ်ပိုင်ကွန်ယက်အတု VPN ကို အသုံးပြုပါ။
- သင့်အိမ်သုံး Wi-Fi ကို ခိုင်မာသော စကားဝှက်ဖြင့် ကာကွယ်ပါ။ ဖြစ်နိုင်ပါက WPA3 ကို အသုံးပြုပါ။
- မလိုအပ်ပါက Wi-Fi၊ Bluetooth နှင့် တည်နေရာဝန်ဆောင်မှုများကို ပိတ်ထားပါ။

- ပွဲများ သို့မဟုတ် ကော်ဖီဆိုင်များတွင် မျှဝေအသုံးပြုသည့် စက်ပစ္စည်းများ သို့မဟုတ် ကွန်ရက်များကို အသုံးပြုရာတွင် သတိထားပါ။

အင်တာနက်ကွန်ယက်လှည့်စား (phishing) တိုက်ခိုက်မှုများကိုသတိထားပါ

- သံသယဖြစ်ဖွယ်လင့်ခ်များကို ဘယ်တော့မှ နှိပ်ခြင်း သို့မဟုတ် မသိသော ပူးတွဲပါဖိုင်များကို ဖွင့်ခြင်း မပြုပါနှင့်။

- မိတ်ဆွေများ သို့မဟုတ် စီစဉ်သူများထံမှ ရောက်လာသည်ဟု ထင်ရသော်လည်း ထူးဆန်းသော တောင်းဆိုမှုများကို အတည်ပြုပါ။

- အကောင့်ဝင်ရောက်ရန် ဟန်ဆောင်ထားသော စာမျက်နှာအတုများနှင့် အရေးတကြီး 'အကောင့်ပိတ်ထားသည်' စသည့် မက်ဆေ့ချ်များကို သတိထားပါ။

- spam နှင့် အင်တာနက်ကွန်ယက်လှည့်စား (phishing) တိုက်ခိုက်မှုများ ကာကွယ်မှုအားကောင်းသော အီးမေးလ်ဝန်ဆောင်မှုပေးသူများကို အသုံးပြုပါ။

မည်သူ ဝင်ရောက်ခွင့်ရှိသည်ကို ထိန်းချုပ်ပါ

- အရေးကြီးသော ဖိုင်များကို တကယ်လိုအပ်သောသူများနှင့်သာ မျှဝေပါ။

- CryptPad သို့မဟုတ် SecureDrop ကဲ့သို့သော ကိရိယာများကို စာရွက်စာတမ်းများ မျှဝေရန် အသုံးပြုပါ။

- အဖွဲ့မှ သို့မဟုတ် ပရောဂျက်မှ တစ်စုံတစ်ဦး ထွက်ခွာသွားသောအခါ ၎င်းတို့၏ ဝင်ရောက်ခွင့်ကို ရုပ်သိမ်းပါ။

- မည်သူက မည်သည့်အရာများကို ဝင်ရောက်ခွင့်ရှိသည်ကို စာရင်းပြုစုထားပါ။

အရန်သိမ်းဆည်းပါ၊ အရန်သိမ်းဆည်းပါ၊ အရန်သိမ်းဆည်းပါ

- အရေးကြီးသော ဖိုင်များကို လုံခြုံစွာ အရန်သိမ်းဆည်းပါ။

- စက်ပစ္စည်းများကို သိမ်းဆည်းခံရပါက၊ ခိုးယူခံရပါက သို့မဟုတ် ထိခိုက်ပျက်စီးပါက အရေးပေါ် စီမံကိန်းတစ်ခု ရှိထားပါ။

- လိုအပ်ပါက သင့်စက်ပစ္စည်းရှိအချက်အလက်များကို အဝေးမှနေ၍ ဖျက်နည်းကို သိထားပါ။

- အရေးကြီးသော အဆက်အသွယ်များနှင့် စီမံကိန်းများ၏ မိတ္တူများကို အင်တာနက်ပြင်တွင်လည်း သိမ်းဆည်းထားပါ။

သင့် နောက်ဆက်တွဲအချက်အလက် (metadata) ကို မမေ့ပါနှင့်

- မျှဝေခြင်းမပြုမီ ဓာတ်ပုံများနှင့် စာရွက်စာတမ်းများမှ နောက်ဆက်တွဲအချက်အလက် (Metadata)ကို ဖယ်ရှားပါ။

- သင့်ကင်မရာနှင့် လူမှုကွန်ရက်အပလီကေးရှင်းများတွင် တည်နေရာထည့်သွင်းခြင်းကို ပိတ်ထားပါ။

- ဓာတ်ပုံများ (screenshots) တွင် အရေးကြီးသောအချက်အလက်များ ပါဝင်နိုင်သည်ကို သတိပြုပါ။

ရုပ်ပိုင်းဆိုင်ရာ လုံခြုံရေးသည်လည်း အရေးကြီးပါသည်

- စက်ပစ္စည်းများကို ရုပ်ပိုင်းဆိုင်ရာအရ လုံခြုံအောင်ထားပါ (သင်နှင့်အတူ သယ်ဆောင်သွားခြင်း သို့မဟုတ် လော့ခ်ချခြင်း)။

- ဆန္ဒပြပွဲများ၊ အစည်းအဝေးများ သို့မဟုတ် ခရီးသွားအချက်အချာနေရာများတွင် စက်ပစ္စည်းများကို ပိုင်ရှင်မဲ့ လက်လွတ်စဖယ်ထားခဲ့ခြင်းမျိုး မလုပ်ပါနှင့်။

- စက်ပစ္စည်းများကို အသုံးမပြုသည့်အခါ ဖန်သားပြင်သော့ခတ်ပြီး လုံးဝပိတ်ထားပါ။

- သင့်ထံ ကမ်းလှမ်းလာသော USB သို့မဟုတ် မည်သည့်စက်ပစ္စည်းများကိုမဆို သတိထားပါ။

- လေ့လာပြီး အသင့်အနေအထားရှိနေပါ
- ဒစ်ဂျစ်တယ်လုံခြုံရေးခြိမ်းခြောက်မှုများနှင့် နည်းဗျူဟာများအကြောင်း နောက်ဆုံးအခြေအနေများကို ဆက်လက်သိရှိနေအောင် လုပ်ပါ။

- သင့်အဖွဲ့သားများနှင့် အသိပညာများကို မျှဝေပါ။

- သင့်အတွက်နှင့် သင့်လုပ်ငန်းအတွက် မည်သည့်အန္တရာယ်များ ရှိနေသည်ကို သိရှိရန် အန္တရာယ်ပုံစံ သတ်မှတ်ခြင်း (threat modeling) ကို လေ့ကျင့်ပါ။

- ယုံကြည်ရသော ဒစ်ဂျစ်တယ်လုံခြုံရေး မဟာမိတ်များ သို့မဟုတ် အဖွဲ့အစည်းများနှင့် ဆက်ဆံရေး တည်ဆောက်ပါ။

သင်ထောက်ကူ အရင်းအမြစ်များ

အရင်းအမြစ်များ	အင်တာနက်စာမျက်နှာ
CiviCERT ဒီဂျစ်တယ် ရှေးဦးသူနာပြုစု ကိရိယာ	https://digitalfirstaid.org/
Electronic Frontiers Foundation ရဲ့ အွန်လိုင်းပေါ်မှာ ကိုယ့်ကိုယ်ကိုယ် စောင့်ကြည့်ခံရတာကနေ ဘယ်လိုကာကွယ်ရမယ်ဆိုတာကို ရှင်းပြထားတဲ့ အရင်းအမြစ်တစ်ခု	https://ssd.eff.org
Front Line Defenders ရဲ့ အကာအကွယ်ပေးရေး လမ်းညွှန်စာအုပ်	https://www.frontlinedefenders.org/en/resource-publication/protection-handbook-human-rights-defenders
Tactical Tech	https://tacticaltech.org/resources/
Security in a Box	https://securityinabox.org/en/
Holistic Security – Tactical Tech	https://holistic-security.tacticaltech.org/ckeditor_assets/attachments/61/hs_complete_hires.pdf
Cyberwomen ရဲ့ အမျိုးသမီး လူ့အခွင့်အရေးကာကွယ်သူများအတွက် ဘက်စုံ ဒစ်ဂျစ်တယ် လုံခြုံရေး သင်ရိုးညွှန်းတမ်း"	https://cyber-women.com/intro/intro.pdf
Blueprints for Change ရဲ့ ဒစ်ဂျစ်တယ်လုံခြုံရေး အခြေခံများ	https://docs.google.com/document/d/1skNzkvS3NcdDeHqzguOI6FfWxuCsOsKyCl8c8aNxzY8/edit?tab=t.0
Digisec.wiki	https://en.digisec.wiki/wiki/Main_Page
Totem project	https://totem-project.org/
စတားလိုက် အားကစားကွင်း - အွန်လိုင်းဂိမ်း (Starlight Stadium – onlinge game)	https://freedomlab.io/wp-content/uploads/2025/02/Starlight-Stadium-Overview-Use-Transferability.pdf
Level Up ရဲ့ ဒစ်ဂျစ်တယ် ဘေးကင်းလုံခြုံရေးအတွက် အရင်းအမြစ်များ	https://www.level-up.cc/

ကိုးကားစာရင်း

Akoto, Michael. “Understanding the Investigatory Encryption Backdoor Debate.” *The Alliance for Citizen Engagement*, January 26, 2025. https://ace-usa.org/blog/research/research-technology/understanding-the-investigatory-encryption-backdoors-debate/

Amnesty International. “The Hidden Victims of Repression – How Activists and Reporters Can Protect Themselves from Secondary Trauma.” Published February 20, 2019. https://www.amnesty.org/en/latest/news/2019/02/how-activists-and-reporters-can-protect-themselves-from-secondary-trauma/.

Amnesty International. *Philippines: “I Turned My Fear into Courage”: Red-Tagging and State Violence Against Young Human Rights Defenders in the Philippines*. Amnesty International, 2024. https://www.amnesty.org/en/documents/asa35/8574/2024/en/.

Amnesty International. “Partners and Support.” Accessed May 13, 2025. https://securitylab.amnesty.org/partners-and-support/.

Avey, Chester. “What to Know About EXIF Data, a More Subtle Cybersecurity Risk.” *ISACA*, February 6, 2025. https://www.isaca.org/resources/news-and-trends/industry-news/2025/what-to-know-about-exif-data-a-more-subtle-cybersecurity-risk.

Awati, Rahul, and Andrew Froehlich. “What Is Elliptical Curve Cryptography (ECC)?” *TechTarget*, March 17, 2025. https://www.techtarget.com/searchsecurity/definition/elliptical-curve-cryptography.

Badman, Annie, and Matthew Kosinski. “What Is Asymmetric Encryption?” *IBM*, August 8, 2024. https://www.ibm.com/think/topics/asymmetric-encryption.

Badman, Annie, and Matthew Kosinski. “What Is Symmetric Encryption?” *IBM*, August 5, 2024. https://www.ibm.com/think/topics/symmetric-encryption

Bagnell, Jason. *NO Microsoft Account Needed! Windows 11 Setup Bypass (LATEST 6/2025).* YouTube video, June 5, 2025. https://www.youtube.com/watch?v=SiDLgdbFdtM.

Bambauer, Derek E. “Privacy Versus Security.” *Journal of Criminal Law and Criminology* 103, no. 3 (2013): 667–84.

Battat, Randy. “End-to-End Encryption: What It Is & How It Works.” *Preveil*, August 30, 2024. https://www.preveil.com/blog/end-to-end-encryption/.

Bhatt, Hemant. “What Is RSA? How Does an RSA Work?” *Encryption Consulting*, March 4, 2024. https://www.encryptionconsulting.com/education-center/what-is-rsa/.

Bhuiyan, Johana. “How to Protect Your Phone and Data Privacy at the US Border.” *The Guardian*, March 26, 2025. https://www.theguardian.com/technology/2025/mar/26/phone-search-privacy-us-border-immigration.

Biddle, Sam. “Facebook Report Concludes Company Censorship Violated Palestinian Human Rights.” *The Intercept*, September 21, 2022. https://theintercept.com/2022/09/21/facebook-censorship-palestine-israel-algorithm/.

Bingham, Brock. “How to Identify and Remove Bloatware from Windows 11.” *PDQ*, December 24, 2024. https://www.pdq.com/blog/how-to-remove-bloatware/.

Blueprints for Change. *How-to Draft: Digital Security Basics for Campaigners*. Blueprints for Change, 2018. https://docs.google.com/document/d/1skNzkvS3NcdDeHqzguOI6FfWxuCsOsKyCl8c8aNxzY8/edit?tab=t.0.

Buckbee, Michael. “What Is a Proxy Server and How Does It Work?” *Varonis* (blog), June 24, 2022. https://www.varonis.com/blog/what-is-a-proxy-server.

Buckbee, Michael. “What Is PGP Encryption and How Does It Work?” *Varonis*, June 2, 2023. https://www.varonis.com/blog/pgp-encryption.

Canadian Centre for Cybersecurity. “Domain Name System (DNS) Tampering – ITSAP.40.021.” cyber.gc.ca, August 2022. https://www.cyber.gc.ca/en/guidance/domain-name-system-dns-tampering-itsap40021.

Canadian Mental Health Association. “Mental Health and Self-Care for Activists.” Accessed May 17, 2025. https://cmha-yr.on.ca/mental-health-and-self-care-for-activists/ .

Citizen Lab. *Everyone’s Guide to Bypassing Internet Censorship*. The Citizen Lab, 2007. https://citizenlab.ca/guides/everyones-guide-english.pdf.

Computer Professionals’ Union. “#Eleksyon2025Watch — RED-HANDED: Report on Social Media Red-Tagging During the Election Period.” *Facebook*, May 18, 2025. https://www.facebook.com/story.php?story_fbid=1130518759115014&id=100064707008190&_rdr.

Cope, Sophia, Amul Kalia, Seth Schoen, and Adam Schwartz. *Digital Privacy at the U.S. Border: Protecting the Data On Your Devices*. Electronic Frontier Foundation, 2017. https://www.eff.org/files/2018/01/11/digital-privacy-border-12-2017.pdf.

Crider, Michael. “Digital Fingerprinting: The Secret, Insidious Way You’re Tracked Online.” *PCWorld*, April 13, 2023. https://www.pcworld.com/article/1684308/what-is-a-digital-fingerprint.html.

Cyberwomen. *Holistic Digital Security Training Curriculum for Women Human Rights Defenders*. Cyberwomen, 2019. https://cyber-women.com/intro/intro.pdf.

Daemen, Joan, and Vincent Rijmen. *The Design of Rijndael: AES — The Advanced Encryption Standard*. Berlin: Springer-Verlag, 2002. https://doi.org/10.1007/978-3-662-60769-5

Day, Brittany. “The Importance of Strong Encryption in Digital Privacy and Security.” *Linux Security* (blog), January 7, 2020. https://linuxsecurity.com/features/encryption-an-essential-yet-highly-controversial-component-of-digital-security.

DigitalHygiene.net. “What Is Digital Hygiene?” Accessed May 10, 2025. https://digitalhygiene.net/.

Digisec.wiki. “Main Page.” Accessed June 15, 2025. https://en.digisec.wiki/wiki/Main_Page.

Doran, Matthew, and Henry Belot. “Australian Federal Police Accessed Journalists' Metadata, Stoking New Media Freedom Concerns.” *ABC*, July 9, 2019. https://www.abc.net.au/news/2019-07-09/afp-access-journalist-metadata-60-times-in-12-months/11290888.

EFF (Electronic Frontier Foundation). “How to: Understand and Circumvent Network Censorship.” Surveillance Self-Defense. Last modified February 01, 2024. https://ssd.eff.org/module/understanding-and-circumventing-network-censorship.

EFF (Electronic Frontier Foundation). “Threat Model.” Surveillance Self-Defense. Accessed June 13, 2025. https://ssd.eff.org/glossary/threat-model.

EFF (Electronic Frontier Foundation). “Your Security Plan.” Surveillance Self-Defense. Published October 27, 2023. https://ssd.eff.org/module/your-security-plan.

eylenburg. “Comparison of Android-Based Operating Systems. *Eylenburg.github.io* (blog). Accessed June 15, 2025. https://eylenburg.github.io/android_comparison.htm.

eylenburg. “Sitemap – Eylenburg.github.io.” *Eylenburg.github.io* (blog). Accessed June 15, 2025. https://eylenburg.github.io/os_comparison.htm.

Federal Bureau of Investigation. “Warrant-Proof Encryption and Lawful Access.”fbi.gov. Accessed April 10, 2025. https://www.fbi.gov/how-we-investigate/lawful-access.

Fingerprint. “Canvas Fingerprinting: What It Is and How It Works.” Accessed June 17, 2025. https://fingerprint.com/blog/canvas-fingerprinting/.

Fuchs, Christian. “Societal and Ideological Impacts of Deep Packet Inspection Internet Surveillance.” *Information, Communication & Society* 16, no. 8 (2013): 1328–59. https://doi.org/10.1080/1369118X.2013.770544.

Frontline Defenders. “About Us.” frontlinedefenders.org. Accessed May 17, 2025. https://www.frontlinedefenders.org/en/who-we-are.

Front Line Defenders. “Emergency Contact for Human Rights Defenders.” Accessed May 23, 2025. frontlinedefenders.org. https://www.frontlinedefenders.org/en/emergency-contact-human-rights-defenders.

FreedomLab. “Starlight Stadium: Overview.” freedomlab.io. Accessed May 16, 2025. https://freedomlab.io/starlight-stadium/.

Fuchs, Christian. “Societal and Ideological Impacts of Deep Packet Inspection Internet Surveillance.” *Information, Communication & Society* 16, no. 8 (2013): 1328–59. https://doi.org/10.1080/1369118X.2013.770544.

(GEC) Global Encryption Coalition admin. “Edward Snowden and the Global Encryption Coalition Say ‘Meddling with Strong Encryption Puts Public and Economy at Risk.’” *Global Encryption Coalition.* Published October 21, 2021. https://www.globalencryption.org/2021/10/edward-snowden-and-the-global-encryption-coalition-say-meddling-with-strong-encryption-puts-public-and-economy-at-risk-press-release/.

Goldberg, Jeffrey, and Shane Harris. “Here Are the Attack Plans That Trump’s Advisers Shared on Signal.” *The Atlantic*, March 25, 2025. https://www.theatlantic.com/politics/archive/2025/03/signal-group-chat-attack-plans-hegseth-goldberg/682176/.

Hanna. “Digital Fingerprinting: Google Launched a New Era of Tracking, but You Can Fight for Your Privacy!” *Tuta*, February 18, 2025. https://tuta.com/blog/digital-fingerprinting-worse-than-cookies.

Human Rights Watch. *Meta’s Broken Promise: Systemic Censorship of Palestine Content on Instagram and Facebook*. Human Rights Watch, 2023. https://www.hrw.org/report/2023/12/21/metas-broken-promises/systemic-censorship-palestine-content-instagram-and.

International Telecommunication Union. *Data Networks, Open System Communications and Security – Telecommunication Security*. International Telecommunications Union, 2008. https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.1205-200804-I!!PDF-E&type=items.

Internet Society. “Internet Shutdowns.” Pulse Internet Society. Accessed June 15, 2025. https://pulse.internetsociety.org/en/shutdowns/?search=HM.

Irwin, Kate. “Worried About Digital Privacy? VPNs and Tor Aren't Enough Anymore.” *PC Mag*, November 4, 2024. https://www.pcmag.com/news/chelsea-manning-vpns-and-tor-arent-enough-for-digital-privacy.

Jancer, Matt. “Proton Says It’ll Leave Switzerland if This Controversial Law Is Passed.” *Vice*, May 15, 2025. https://www.vice.com/en/article/proton-says-it-will-leave-switzerland-if-controversial-swiss-law-passes/.

Knodel, Mallory, et al. “Five Eyes Campaign Against Encryption Threatens Democracy.” *Tech Policy Press*, October 11, 2023. https://www.techpolicy.press/five-eyes-campaign-against-encryption-threatens-democracy/.

Lorentzen, Linus. “What Is V2Ray, and How Does It Work?” *Doprax* (blog), June 21, 2023. https://www.doprax.com/privacy/what-is-v2ray-and-how-can-you-use-it/.

Luciano, Dennis, and Gordon Prichett. “Cryptology: From Caesar Ciphers to Public-Key Cryptosystems.” *The College Mathematics Journal* 18, no. 1 (1987): 2–17. https://www.tandfonline.com/doi/abs/10.1080/07468342.1987.11973000.

Mann, Steve. “Sousveillance: Secrecy, Not Privacy, May Be the True Cause of Terrorism.” 2002. Accessed June 10, 2025. http://www.wearcam.org/sousveillance.htm.

Mendelson, Allegra. “Cat and Mouse: Myanmar Netizens Find Cracks in Draconian VPN Ban.” *Frontier Myanmar*, August 6, 2024. https://www.frontiermyanmar.net/en/cat-and-mouse-myanmar-netizens-find-cracks-in-draconian-vpn-ban/.

Monahan, Torin. “On the Impossibility of Ethical Surveillance.” In *The Handbook of Communication Ethics*, edited by Amit Pinchevski, Patrice M. Buzzanell, and Jason Hannan. Routledge, 2022. http://dx.doi.org/10.2139/ssrn.4129499.

Mullvad. “Introducing Shadowsocks Obfuscation for WireGuard.” Published October 25, 2024. https://mullvad.net/en/blog/introducing-shadowsocks-obfuscation-for-wireguard.

Mullin, Joe, and Cindy Cohn. “Salt Typhoon Hack Shows There's No Security Backdoor That's Only for the ‘Good Guys.’” *Electronic Frontier Foundation*, October 9, 2024. https://www.eff.org/deeplinks/2024/10/salt-typhoon-hack-shows-theres-no-security-backdoor-thats-only-good-guys.

Myanmar Internet Project. “Digital Coup Timeline.” Accessed June 16, 2025. https://www.myanmarinternet.info/.

Negroponte, Nicholas. *Being Digital*. 1st Edition. Knopf, 1995.

OpenPGP. “About.” Last modified September 29, 2024. https://www.openpgp.org/about/.

Phiffer, Dan, Tomas Apodaca, Miles Hilton, and Maddy Varner. “How Do I Prepare My Phone for a Protest? (Updated 2024).” *The Markup*, May 4, 2024. https://themarkup.org/the-breakdown/2024/05/04/how-do-i-prepare-my-phone-for-a-protest-updated-2024.

Pines, Christopher. *Ideology and False Consciousness: Marx and His Historical Progenitors*. SUNY Press, 1993.

Podus. “Access to Justice Empowering Justice, Connecting Lives.” podus.org. Accessed June 16, 2025. https://podus.org/.

Poggi, Nicolas. “Encryption Choices: RSA vs. AES Explained.” *Prey Project* (blog), June 2, 2025. https://preyproject.com/blog/types-of-encryption-symmetric-or-asymmetric-rsa-or-aes.

Privacy Guides. “Onion Browser Review: Tor on iOS.” privacyguides.org. Accessed June 15, 2025. https://www.privacyguides.org/articles/2024/09/18/onion-browser-review/.

Privacy Guides. “The Collaborative Privacy Advocacy Community.” Accessed April 20, 2025. https://www.privacyguides.org/en/.

Privacy Guides. “Android Overview.” Accessed June 24, 2025. https://www.privacyguides.org/en/os/androidoverview/#safetynet-and-play-integrity-api.

Privacy Guides. “iOS Overview.” Accessed June 24, 2025. https://www.privacyguides.org/en/os/ios-overview/.

Privacy Tools. “Privacy Tools Guide: Website for Encrypted Software & Apps.” https://www.privacytools.io/.

ProtonVPN. “Defeat Censorship with Stealth, Our New VPN Protocol.” protonvpn.com. October 6, 2022. https://protonvpn.com/blog/stealth-vpn-protocol.

Rahman-Jones, Imran. “Microsoft Rolls Out AI Screenshot Tool Dubbed 'Privacy Nightmare.'” *BBC News*, April 11, 2025. https://www.bbc.com/news/articles/cj3xjrj7v78o.

Ramirez, Araceli. “IMSI Catchers in Paraguay: The Invisible Surveillance Threatening Your Right to Protest.” *TEDIC*, May 19, 2025. https://www.tedic.org/en/imsi-catchers-in-paraguay-the-invisible-surveillance-threatening-your-right-to-protest/.

Sammut, Tim. “Secure Communications Framework.” *Teamsammut* (blog), March 4, 2016. https://teamsammut.com/scf/.

Saravasti, NT. “How India’s Police Is Using Metadata.” *Medianama*, November 23, 2023. https://www.medianama.com/2023/11/223-india-police-metadata-use-tracking-2/.

Security in a Box. “What Do You Need to Protect?” Accessed June 16, 2025. https://securityinabox.org/en/.

Schneider, Josh, and Ian Smalley. “What Is Public Key Infrastructure?” *IBM*, August 12, 2024. https://www.ibm.com/think/topics/public-key-infrastructure.

SHARE Foundation, Hermes Center, Bits of Freedom, ARTICLE19, Homo Digitalis, and EDRi. *Campaign “Reclaim Your Face” Calls for a Ban on Biometric Mass Surveillance*. EDRi, November 12, 2020. https://edri.org/our-work/campaign-reclaim-your-face-calls-for-a-ban-on-biometric-mass-surveillance/.

Smith, Serena. “We Spend 88 Days a Year on Our Phones.” *Dazed*, April 25, 2025. https://www.dazeddigital.com/life-culture/article/66669/1/we-spend-88-days-a-year-on-our-phones-addiction-mental-health-loneliness.

SSL Support Team. “What Is Certificate Authority (CA)?” *SSL.com*, January 5, 2024. https://www.ssl.com/article/what-is-a-certificate-authority-ca/.

Tamuliunaite, Vejune. “SOCKS vs HTTP Proxy: What Is the Difference?” *Oxylabs*, May 30, 2025. https://oxylabs.io/blog/socks-vs-http-proxy.

Tashea, Jason. “Stay Safe Out There: Threat Modeling for Campaigners.” *Mobilisation Lab*, August 12, 2015. https://mobilisationlab.org/stories/threat-modeling-for-campaigners-and-activists/.

Tactical Technology Collective. *Holistic Security: A Strategy Manual for Human Rights Defenders*. Tactical Technology Collective, 2016. https://holistic-security.tacticaltech.org/ckeditor_assets/attachments/61/hs_complete_hires.pdf.

Tor Project. “Is Tor Browser Available on F-Droid?” support.torproject.org . Accessed June 15, 2025. https://support.torproject.org/tormobile/tormobile-7/.

Totem. “What Is Totem?” totem-project.org. Accessed May 10, 2025. https://totem-project.org/.

Vigderman, Aliza and Gabe Turner. “Internet Censorship in 2025: The Impact of Internet Restrictions.” *Security.org*. Last modified August 22, 2024. https://www.security.org/vpn/internet-censorship/.

Ververis, Vasilis. “Internet Censorship in the European Union.” PhD thesis, School of Business and Economics of Humboldt-Universität zu Berlin, 2022. https://edoc.hu-berlin.de/server/api/core/bitstreams/1d147948-861e-4a1f-9baf-b81bc786f06a/content.

Whittaker, Meredith (meredith-signal). “Help People in Iran Reconnect to Signal – A Request to Our Community.” *Signal.org* (blog), September 22, 2022. https://signal.org/blog/run-a-proxy/.

Wothaya, Jacinta. “What Is Censorship and What Tools Can SJOs Use to Bypass Restricted Content?” *Tatua Digital Resilience Centre*, September 2, 2024. https://tatua.digital/services/what-is-censorship-and-what-tools-can-sjos-use-to-bypass-restricted-content/.

Woodhams, Samuel. “The Rise of Internet Throttling: A Hidden Threat to Media Development.” *Center for International Media Assistance*, May 20, 2020. https://www.cima.ned.org/publication/the-rise-of-bandwidth-throttling-a-hidden-threat-to-media-development/.

York, Jillian C. “The Right to Anonymity Is Vital to Free Expression: Now and Always.” *Electronic Frontier Foundation*, March 25, 2020. https://www.eff.org/deeplinks/2020/03/right-anonymity-vital-free-expression-now-and-always.

Zuboff, Shoshana. *The Age of Surveillance Capitalism*. PublicAffairs, 2019.