EFF'S SURVEILLANCE SELF-DEFENSE

လူမှုကွန်ယက်များပေါ်မှာ မိမိကိုယ်ကိုကာကွယ်ခြင်း

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

LOCALIZATION LAB

လူမှုကွန်ယက်များပေါ်မှာ မိမိကိုယ်ကိုကာကွယ်ခြင်း

နောက်ဆုံးစိစစ်ထားသည့်ရက်စွဲ - ၂၀၂၁ ခုနှစ် ဇွန်လ ၂၅ ရက်

လူမှုကွန်ယက်တွေဟာ အင်တာနက်ပေါ်က လူသုံးအများဆုံး ဝက်ဘ်ဆိုဒ်တွေထဲမှာ ပါဝင်ပါတယ်။ လူမှုကွန်ယက် တစ်ခုဖြစ်တဲ့ ဖေ့စ်ဘုခ် Facebook မှာ သုံးစွဲသူပေါင်း သန်းတစ်ထောင်ကျော်ရှိပါတယ်။ အင်စတာဂရမ် Instagram နဲ့ တွစ်တာ Twitter တွေမှာ သုံးစွဲသူပေါင်း သန်းရာနဲ့ချီပြီး ရှိပါတယ်။ စတင်တည်ထောင်ချိန်မှာ post ရေးတင်ဖို့၊ ဓာတ်ပုံများနှင့် ကိုယ်ရေးအချက်အလက်တွေ မျှဝေဖို့ ရည်ရွယ်ခဲ့ပါတယ်။ အခုအချိန်မှာတော့ လူအများကြား စည်းရုံးလှုံ့ဆော်ဖို့လည်း အသုံးပြုလာကြပါတယ်။ ဘာကိစ္စအတွက်ဘဲသုံးသုံး ကိုယ်ရေးကိုယ်တာလျှို့ဝှက်မှုနဲ့ အမည်ဝှက်ထားရှိနိုင်မှုတို့ဟာ အရေးကြီးပါတယ်။

ဒါကြောင့် လူမှုကွန်ယက်တွေကို အသုံးပြုတဲ့အခါမှာ အခုဖော်ပြထားတဲ့မေးခွန်းတွေကို အရင်ဆန်းစစ်ဖို့ လိုပါတယ် - ဒီဝက်ဘ်ဆိုဒ်တွေကို သုံးနေစဉ်မှာ ကိုယ့်ကိုယ်ကို ဘယ်လိုကာကွယ်နိုင်မလဲ၊ အခြေခံ ကိုယ်ရေးကိုယ်တာ လျှို့ဝှက်လုံခြုံမှု ဘယ်လိုရှိမလဲ၊ မိမိဘယ်သူဘယ်ဝါဖြစ်တယ်ဆိုတာ ဘယ်လိုကာကွယ်ရမလဲ၊ မိမိရဲ့ အဆက်အသွယ်တွေနဲ့ ပတ်သက်သူတွေကိုကော ဘယ်လိုကာကွယ်ရမလဲ၊ ဘယ်လို သတင်းအချက်အလက်တွေကို ကိုယ်ရေးကိုယ်တာ အနေနဲ့ လျှို့ဝှက်ထားပြီး ဘယ်သူတွေဆီကနေ လျှို့ဝှက်ထားရမလဲ။

ကိုယ့်ရဲ့အခြေအနေအပေါ်မူတည်ပြီးတော့ လူမှုကွန်ယက်ကုမ္ပဏီဆီကနေရော၊ အခြားသုံးစွဲသူများဆီကနေပါ မိမိ ကိုယ်ကို ကာကွယ်ဖို့ လိုအပ်နိုင်ပါတယ်။

အကောင့်အသစ်ဖန်တီးတဲ့အခါ ဂရုပြုရန် အချက်များ

- ကိုယ့်ရဲ့ **အမည်အရင်း** ကို အသုံးပြုချင်သလား။ အချို့လူမှုကွန်ယက်တွေမှာ “အမည်အရင်းအသုံးပြုရန် သတ်မှတ်ချက်” ထားရှိတတ်ပေမယ့် တင်းတင်းကြပ်ကြပ်လိုက်နာကျင့်သုံးစရာ မလိုပါဘူး။ လူမှုကွန်ယက် အသုံးပြုဖို့ မှတ်ပုံတင်တဲ့အခါ အမည်အရင်းမသုံးချင်ဘူးဆိုရင် မသုံးပါနဲ့။
- မှတ်ပုံတင်တဲ့အခါမှာ လိုအပ်တဲ့အချက်အလက်ထက် ပိုမဖြည့်ပါနဲ့။ ကိုယ်ဘယ်သူလဲဆိုတာ လျှို့ဝှက်ထား ချင်တယ်ဆိုရင် သီးသန့် **အီးမေးလ်လိပ်စာ** တစ်ခု ဖန်တီးအသုံးပြုပါ။ ကိုယ်ရဲ့

ဖုန်းနံပါတ် ကို မပေးပါနဲ့။ ဒီ အချက်အလက်နှစ်မျိုးစလုံးဟာ ကိုယ်ဘယ်သူဘယ်ဝါဖြစ်တယ်ဆိုတာနဲ့ တိုက်ရိုက် ချိတ်နေတာဖြစ်လို့ အကောင့်တွေခွဲပြီးသုံးနေရင်တောင် ကိုယ်တစ်ဦးတည်းကသုံးနေတာဖြစ်ကြောင်း ရှာဖွေဖော်ထုတ်နိုင်ပါ စေလိမ့်မယ်။

- **ပရိုဖိုင်ဓာတ်ပုံ သို့မဟုတ် ရုပ်ပုံ**ရွေးတဲ့အခါ သတိထားပါ။ ဓာတ်ပုံတစ်ပုံကို ဘယ်အချိန် ဘယ်နေရာမှာ ရိုက်ခဲ့သလဲ ဆိုတာကို အချက်အလက်အကြောင်းရှင်းပြတဲ့ နောက်ခံအချက်အလက် (metadata) ကနေ သိနိုင်တဲ့အပြင် မိမိတင်တဲ့ဓာတ်ပုံတွေကနေလည်း မိမိအကြောင်းကို စုံစမ်းသိရှိစေနိုင်ပါတယ်။ ဒါကြောင့် ပုံတင်ဖို့ ဓာတ်ပုံရွေးတဲ့အခါ ကိုယ့်အိမ်၊ အလုပ်စတဲ့နေရာတွေအနီးမှာ ရိုက်ထားတဲ့ပုံဖြစ်နေသလား၊ လိပ်စာနဲ့လမ်းနာမည်စတာတွေကို မြင်ရသလား ဆန်းစစ်ပါ။
- လူမှုကွန်ယက်အသုံးပြုဖို့ မှတ်ပုံတင်တဲ့အခါ မိမိရဲ့ IP လိပ်စာ ကိုတစ်ပါတည်း မှတ်ထားနိုင်တယ်ဆိုတာ သတိပြုပါ။
- ခိုင်ခံ့လုံခြုံတဲ့ စကားဝှက် ရွေးချယ် အသုံးပြုပါ။ ဖြစ်နိုင်ရင် အဆင့်နှစ်ဆင့်ဖြင့်စစ်မှန်ကြောင်း သက်သေ ပြခြင်း စနစ်ကို အသုံးပြုပါ။
- စကားဝှက် မေ့သွားရင် အသစ်ပြန်ပြောင်းတဲ့အခါ သုံးဖို့ထားတဲ့မေးခွန်းတွေကို သတိထားဖြေပါ။ “သင် ဘယ်မြို့ မှာမွေးတာလဲ” သို့မဟုတ် “သင့်ရဲ့ခွေးနာမည်ဘာလဲ” ဆိုတဲ့မေးခွန်းတွေရဲ့ အဖြေကို အပြင်လူ တစ်ယောက်က မိမိရဲ့ လူမှုကွန်ယက်ပေါ်ကနေ ရှာဖွေသိရှိနိုင်လို့ပါ။ ဒါကြောင့်အဖြေမှန်မဖြေဖို့ အကြံပြု လိုပါတယ်။ အဖြေမှန်မသုံးလို့ ဒီမေးခွန်းတွေမှာ ကိုယ်ဘယ်လိုဖြေခဲ့သလဲ မေ့သွားမှာစိုးရိမ်တယ်ဆိုရင် ကိုယ်သုံးခဲ့တဲ့အဖြေကို စကားဝှက်များသိမ်းဆည်းနိုင်သည့်နေရာ တွင် ထည့်သိမ်းထားနိုင်ပါတယ်။

လူမှုကွန်ယက်ရဲ့ ကိုယ်ရေးကိုယ်တာလုံခြုံမှုဆိုင်ရာ မူဝါဒများကို လေ့လာပါ

သတင်းအချက်အလက်သိုလှောင်သိမ်းဆည်းတဲ့ ကုမ္ပဏီတွေဟာ သူတို့ချမှတ်ထားတဲ့ ကိုယ်ရေးကိုယ်တာလုံခြုံမှု ဆိုင်ရာမူဝါဒတွေအရ ဒီအချက်အလက်တွေကို အသုံးပြုခွင့်ရှိပါတယ်။ ဒါကြောင့် အချက်အလက်တွေကို စီးပွားရေး ဆိုင်ရာကိစ္စများအတွက် အသုံးချတာ၊ ဈေးကွက်မြှင့်တင်တဲ့ မားကတ်တင်းကုမ္ပဏီလိုမျိုး အခြားအဖွဲ့အစည်းတွေ ထံ ပြန်ရောင်းတာတွေ လုပ်နိုင်ပါတယ်။ ကိုယ်ရေးကိုယ်တာလုံခြုံမှု ဆိုင်ရာမူဝါဒတွေအားလုံးကို လိုက်ဖတ်ဖို့ မဖြစ်နိုင်ပေမယ့်လည်း ဖတ်သင့်တဲ့အပိုင်းတစ်ချို့ရှိပါတယ်။ မိမိရဲ့အချက်အလက်တွေကို ဘယ်လိုအသုံးချသလဲ၊ အခြားအဖွဲ့အစည်းများနဲ့ ဘယ်လိုမျှဝေသုံးစွဲသလဲ၊ စုံစမ်းထောက်လှမ်းရေး၊ ရဲ စတဲ့အစိုးရအဖွဲ့များက အချက် အလက်တွေ ကိုတောင်းခံလာရင် ဘယ်လိုတုံ့ပြန်သလဲ ဆိုတဲ့အပိုင်းတွေကို သေသေချာချာဖတ်ရှုသင့်ပါတယ်။

လူမှုကွန်ယက်တွေဟာ အများအားဖြင့် အကျိုးအမြတ်ရရှိဖို့ တည်ဆောက်ထားတဲ့လုပ်ငန်း တွေဖြစ်ကြတဲ့အတွက် ကိုယ့်ဆီကသတင်းအချက်အလက်တွေကို အသုံးချနိုင်ဖို့ ရနိုင်သမျှ

ကောက်ယူလေ့ရှိပါတယ်။ ကိုယ်က မဖြည့် ထားတဲ့ အရေးကြီးအချက်အလက်တွေကိုတောင် ရယူနိုင်ပါတယ်။ ဥပမာ ကိုယ်ဘယ်မှာရှိနေတယ်၊ ဘယ်လို အွန်လိုင်းကြော်ငြာတွေကို ကြည့်ဖြစ်တယ်၊ တခြားဘယ်ဝက်ဘ်ဆိုဒ်တွေကို တက်ကြည့်ဖူးတယ် ဆိုတာတွေကို “Like” ခလုတ်နှိပ်တာကနေခြေရာခံခြင်း စသည်ဖြင့်ပြုလုပ်ပြီး သိရှိနိုင်ပါတယ်။ ဒါကြောင့် ကိုယ့်ကိုမှတ်မိအောင် ခြေရာခံဖို့ အခြားအဖွဲ့များကသုံးတဲ့ ကွတ်ကီး လိုဆော့ဖ်ဝဲတွေကို ပိတ်ပင် ထားသင့်ပါတယ်။ ဒါအပြင် သတင်း အချက်အလက်တွေ မပေါက်ကြားအောင် ခြေရာခံမှုပိတ်ပင်ပေးတဲ့ browser extension တွေကို သုံးသင့်ပါတယ်။

ကိုယ်ရေးကိုယ်တာဆိုင်ရာ အစီအမံများကို ပြောင်းလဲပါ

ပိုပြီးတိတိကျကျပြောရရင် နဂိုအတိုင်းပါလာတဲ့ အစီအမံတွေ (default settings) ကို ပြောင်းလဲပစ်ပါ။ ဥပမာ ကိုယ်တင်တဲ့ post တွေကို လူတိုင်းကြည့်လို့ရအောင် မျှဝေချင်သလား၊ ကိုယ့်အသိအကျွမ်းတွေဘဲ ကြည့်လို့ရ အောင်ထားချင်သလား။ ကိုယ့်အီးမေးလ်လိပ်စာ သို့မဟုတ် ဖုန်းနံပါတ်ကို မျှဝေချင်သလား။ ကိုယ်ဘယ်နားမှာ ရောက်နေတယ်ဆိုတဲ့ သတင်းအချက်အလက်ကို အခြားသူများသိရှိနိုင်အောင် အလိုအလျောက် မျှဝေချင်သလား။ ကိုယ့်ရွေးချယ်မှုအပေါ်မူတည်ပြီး အစီအမံတွေကို သွားပြောင်းပါ။

လူမှုကွန်ယက်တွေရဲ့ အစီအမံတွေ (settings) ဟာ တစ်ခုနဲ့တစ်ခု မတူဘူးဆိုပေမယ့်လည်း ဘုံပါဝင်တဲ့ အချက် အချို့လည်းရှိပါတယ်။

- **ကိုယ်ရေးကိုယ်တာလုံခြုံမှု** အစီအမံတွေမှာဆိုရင် “ဘာကို ဘယ်သူက မြင်တွေ့ခွင့်ရှိသလဲ” ဆိုတဲ့ မေးခွန်း ပါဝင်တတ်ပါတယ်။ အသုံးပြုတဲ့ကွန်ယက်အပေါ်မူတည်ပြီး မြင်တွေ့နိုင်သူတွေ (“အများပြည်သူအားလုံး” “သူငယ်ချင်းတွေနဲ့ သိတဲ့သူတွေ” “သူငယ်ချင်းများသာ” စသည်ဖြင့်)၊ နေရာဒေသ၊ ဓာတ်ပုံများ၊ ဆက်သွယ်ရန်အချက်အလက်၊ tagging ၊ ကိုယ့်ကို လူမှုကွန်ယက်ပေါ်မှာ ဘယ်လိုရှာဖွေတွေ့ရှိနိုင်သလဲ စသည်တို့နဲ့ ပတ်သက်တဲ့ အစီအမံတွေကို တွေ့ရပါလိမ့်မယ်။
- **ဘေးအန္တရာယ်လုံခြုံရေး** ဆိုင်ရာအစီအမံများမှာဆိုရင် အခြားသူများရဲ့ အကောင့်တွေကို ပိတ်ပင်ခြင်း၊ မမြင်ရအောင်ပြုလုပ်ခြင်း၊ အပြင်လူတစ်ယောက်က ကိုယ့်အကောင့်ထဲဝင်ဖို့ကြိုးစားတယ်ဆိုရင် အသိ ပေးအကြောင်းကြားခြင်း စတာတွေနဲ့ပတ်သက်တဲ့ ရွေးချယ်စရာတွေ ပါတတ်ပါတယ်။ တစ်ခါတစ်ရံမှာ အဆင့်နှစ်ဆင့်ဖြင့် စစ်မှန်ကြောင်းသက်သေပြခြင်း သို့မဟုတ် အရန် အီးမေးလ်လိပ်စာ/ဖုန်းနံပါတ်ထား ခြင်း စတဲ့ အကောင့်ထဲဝင်တာနဲ့ ပတ်သက်တဲ့ အစီအမံတွေကိုလည်း ဒီအပိုင်းအောက်မှာ တွေ့ရှိနိုင်ပါ တယ်။ ဒီမှာမရှိရင်တော့ အကောင့်နဲ့ပတ်သက်တဲ့အစီအမံများ သို့မဟုတ် အကောင့်ထဲဝင်ရောက်မှု ဆိုင်ရာ အစီအမံများအောက်မှာ သွားရှာရပါလိမ့်မယ်။
- အဲဒီအပိုင်းတွေမှာ စကားဝှက် ပြောင်းတာနဲ့ ပတ်သက်တဲ့ ကိစ္စတွေလည်း ပါရှိနိုင်ပါတယ်။

ဘေးအန္တရာယ်လုံခြုံရေး နဲ့ ကိုယ်ရေးကိုယ်တာလုံခြုံရေးဆိုင်ရာ **“စစ်ဆေးခြင်း check-up”** များသုံးလို့ရလျှင် အသုံးပြုပါ။ Facebook ၊ Google နဲ့ အခြားဝက်ဘ်ဆိုဒ်အကြီးတွေမှာ “လုံခြုံရေးစစ်ဆေးခြင်း” ဆိုတဲ့ ဝန်ဆောင်မှု ပါရှိတတ်ပါ တယ်။ ဘေးအန္တရာယ်လုံခြုံရေး နဲ့ ကိုယ်ရေးကိုယ်တာလုံခြုံရေးဆိုင်ရာ အသုံးများတဲ့အစီအမံတွေကို နေ့စဉ်သုံး စကားလုံးတွေသုံးပြီး တစ်ဆင့်ချင်းစီ သေသေချာချာရှင်းပြပေးတဲ့အတွက် အသုံးပြုသူတွေအတွက် နားလည်ရ လွယ်ကူစေပါတယ်။

နောက်ဆုံးအနေနဲ့ မှတ်ထားဖို့က ကိုယ်ရေးကိုယ်တာလုံခြုံရေးဆိုင်ရာအစီအမံတွေဟာ ပြောင်းလဲမှုရှိနိုင်တယ် ဆိုတာဖြစ်ပါတယ်။ တစ်ခါတစ်ရံမှာ အစီအမံတွေဟာ ပိုကောင်းလာပြီး လုံခြုံမှုပိုရှိလာနိုင်သလို တစ်ခါတစ်လေ ပိုဆိုးသွားနိုင်ပါတယ်။ ဒါကြောင့် လုံခြုံရေးဆိုင်ရာအစီအမံတွေ ပြောင်းလဲတယ်ဆိုရင် သတိထားဖတ်ပါ။ ယခင်က ဘယ်သူနဲ့မှ မမျှဝေဘဲ လျှို့ဝှက်ထားတဲ့ အချက်အလက်တွေကို အခု အခြားသူတွေနဲ့ မျှဝေဖို့လုပ်နေသလား၊ ယခင် ထက် ပိုပြီးလုံခြုံစေမယ့် အစီအမံအသစ်တွေ ထပ်ထွက်လားသလား ဆိုတာတွေ သတိထားကြည့်ပါ။

မတူညီတဲ့ profile တွေကို ချိတ်ဆက်မှုမလုပ်ဘဲ သီးသန့်ခွဲထားပါ

လူတော်တော်များများမှာ အလုပ်ကိစ္စသုံးတဲ့ profile ၊ dating ဝက်ဘ်ဆိုဒ်တွေမှာ သုံးတဲ့ profile ၊ ဘယ်သူမှမသိ အောင်သုံးတဲ့ အကောင့် ၊ သက်ဆိုင်တဲ့ ပတ်ဝန်းကျင်အသီးသီးမှာ သုံးတဲ့ အကောင့်များ စသည်ဖြင့် profile မျိုးစုံ၊ အကောင့်မျိုးစုံ ရှိနိုင်ပါတယ်။ ဒီလိုမတူညီတဲ့ အကောင့်တွေကို တစ်ခုနဲ့တစ်ခု မချိတ်မိစေဘဲ သီးသန့်ခွဲထားဖို့လို တယ်ဆိုရင် သတိထားဖို့အရေးကြီးပါတယ်။

အထူးသဖြင့် ဖုန်းနံပါတ်နဲ့ ဓာတ်ပုံတွေကို သတိထားပါ။ ကိုယ်မချိတ်မိစေချင်တဲ့ အကောင့်နှစ်ခုမှာ ဓာတ်ပုံအတူ တူသွားတင်မိမယ်ဆိုရင် ဒါဟာကိုယ်တစ်ယောက်တည်းရဲ့အကောင့်ဆိုတာ ချိတ်မိသွားစေမှာ ဖြစ်ပါတယ်။ ဒီကိစ္စ ဟာ dating ဝက်ဘ်ဆိုဒ်တွေနဲ့ အလုပ်ကိစ္စအတွက်အသုံးပြုတဲ့ profile တွေမှာ ပြဿနာအဖြစ်များပါတယ်။ ကိုယ့်ရဲ့အကောင့်ကို လျှို့ဝှက်ထားချင်တယ်၊ အခြားသုံးနေကြအကောင့်တွေနဲ့ ချိတ်ဆက်မှု မရှိစေချင်ဘူးဆိုရင် တခြားဘယ်နေရာမှာမှ မသုံးဖူးတဲ့ ဓာတ်ပုံ/ရုပ်ပုံကို ရွေးသုံးပါ။ မသေချာဘူးဆိုရင် Google ရဲ့ reverse image search ကိုအသုံးပြုပြီး အသုံးပြုမယ့်ဓာတ်ပုံက အွန်လိုင်းတခြားနေရာမှာ ပေါ်လာသလားရှာကြည့်ပါ။ တခြား ချိတ်မိစေ နိုင်တဲ့ အချက်အလက်တွေမှာဆိုရင် မိမိအမည် (အမည်ပြောင်အပါအဝင်) နဲ့ အီးမေးလ်လိပ်စာတို့ ပါဝင်နိုင်ပါ တယ်။ ဒီအချက်အလက်တွေဟာ ကိုယ်သတိမထားမိလိုက်ဘဲ မရှိသင့်တဲ့နေရာမှာ ရောက်နေမယ်ဆို ရင်လည်း အရမ်း မစိုးရိမ်ပါနဲ့။ အင်တာနက်တစ်ခုလုံးပေါ်ကနေ ကိုယ်နဲ့ပတ်သက်တဲ့အကြောင်းအရာအားလုံး ဖျောက်ဖျက်ပစ်ဖို့ ကြိုးစားမယ့်အစား အရေးကြီးတဲ့အချက်အလက်တွေ ဘာတွေရှိတယ်၊ ဘယ်နေရာမှာ တင် ထားတယ်၊ ဘာဆက် လုပ်ရမယ်ဆိုပြီး တစ်ခုချင်းစီခွဲစဉ်းစားပါ။

Facebook အုပ်စုအဖွဲ့များဆိုင်ရာ အစီအမံများနဲ့ ပတ်သက်ပြီး သိထားအောင်ကြိုးစားပါ။

လူမှုရေးလှုပ်ရှားမှု၊ စည်းရုံးလှုံ့ဆော်မှု စတဲ့ အန္တရာယ်များနိုင်တဲ့ကိစ္စတွေအတွက် Facebook အုပ်စုတွေဟာ အလွန်အရေးကြီးတဲ့နေရာတွေ ဖြစ်လာနေပါပြီ။ အုပ်စုအလိုက် Facebook အသုံးပြုမှုနဲ့ဆိုင်တဲ့ အစီအမံတွေဟာ နားလည်ရခက်တာမျိုး ရှိနိုင်ပါတယ်။ ဒါကြောင့် အုပ်စုအဖွဲ့များရဲ့ ကိုယ်ရေးကိုယ်တာလုံခြုံမှုအစီအမံများ နဲ့ မိမိရဲ့ Facebook အုပ်စုအဖွဲ့များ ကိုယ်ရေးကိုယ်တာလုံခြုံမှုနဲ့ ဘေးအန္တရာယ်လုံ ခြုံမှုရှိအောင် အဖွဲ့ဝင်များနဲ့ အတူတကွ ကြိုးပမ်းခြင်း ဆိုတဲ့ လမ်းညွှန်တွေကို ဆက်လက်ကြည့်ရှုပါ။

ကိုယ်ရေးကိုယ်တာလုံခြုံမှုဟာ အားလုံးရဲ့ ပူးပေါင်းပါဝင်မှုလိုအပ်ပါတယ်။

ကိုယ်တစ်ယောက်တည်းရဲ့ လူမှုကွန်ယက် အစီအမံများနဲ့ သုံးစွဲမှုအမူအကျင့်တွေ ပြောင်းလဲလို့မရပါဘူး။ ကိုယ့်ရဲ့ သူငယ်ချင်း အသိမိတ်ဆွေတွေနဲ့ ပြောဆိုပြီး အချင်းချင်းကြား အရေးကြီးတဲ့အချက်အလက်တွေကို အွန်လိုင်းမှာ အမှုမဲ့အမှတ်တဲ့ ပေါက်ကြားမှုမရှိအောင် ဘယ်လိုလုပ်ရမလဲဆိုတာကို ဆွေးနွေးတိုင်ပင်သင့်ပါတယ်။ ကိုယ့်မှာ လူမှုကွန်ယက်အကောင့်မရှိဘူး၊ ကိုယ့်ကို post တွေမှာ tag အလုပ်မခံဘူး ဆိုရင်တောင်မှ သူငယ်ချင်းတွေက ကိုယ်ဘယ်သူလဲ၊ ဘယ်နေရာမှာရှိနေလဲ၊ ကိုယ်နဲ့ဘယ်လိုပတ်သက်နေလဲ ဆိုတာတွေကို အမှုမဲ့အမှတ်မဲ့ ဖော်ထုတ်မိတာမျိုး ဖြစ်ပေါ်နိုင်ပါတယ်။ ကိုယ်ရေးကိုယ်တာအချက်အလက် ကာကွယ်ဖို့ဆိုတာ ကိုယ်တစ်ဦးတည်းဂရုစိုက်ဖို့ပဲမဟုတ်ဘဲ အချင်းချင်း အပြန်အလှန်ဂရုစိုက်ဖို့လည်း လိုပါတယ်။