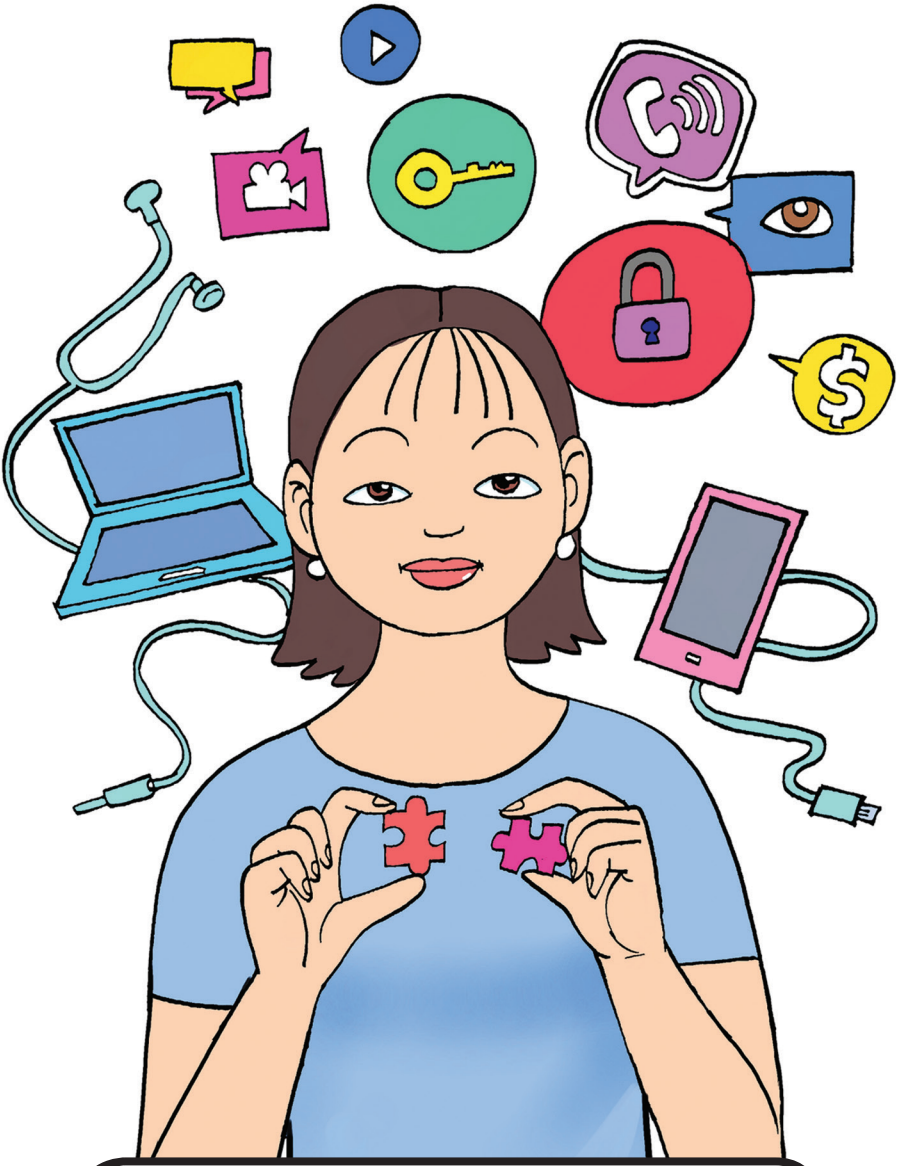
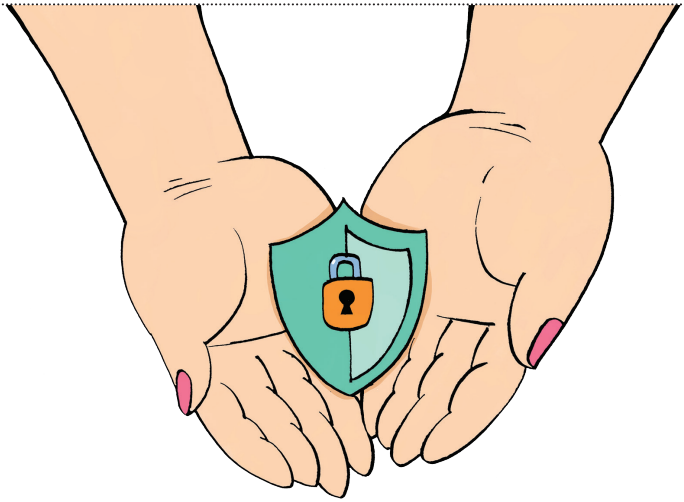


လုံခြုံဘဝညီအမ

မြန်မာအမျိုးသမီးများနှင့် မိန်းကလေးငယ်များ၏
ဒီဂျစ်တယ်လုံခြုံရေးအတွက် လက်တွေ့ဘဝလမ်းညွှန်

https://safesisters.net တွင် လမ်းညွှန်အားရယူပြီး ပိုမိုလေ့လာနိုင်ပါသည်။



ဒီစာအုပ်ငယ်ကလေးက ဘာလဲ

ကျွန်မတို့ရဲ့ စာအုပ်ငယ်ကလေးကို ယူကြည့်တဲ့အတွက် ကျေးဇူးတင်ပါတယ်။ ဒီစာအုပ်ကိုရေးရတဲ့ ရည်ရွယ်ချက်ကတော့ ကျွန်မတို့ရဲ့ ညီအစ်မတွေ အင်တာနက်ပေါ်မှာ ကြုံတွေ့နိုင်တဲ့ပြဿနာတွေ (ကိုယ်ရေးကိုယ်တာဓာတ်ပုံတွေပေါက်ကြားတာ၊ အခိုးခံရတာ၊ ဗိုင်းရပ်စ်တွေနဲ့ အလိမ်အညာဇာတ်လမ်း စတာတွေ) အကြောင်း သိရှိနိုင်စေဖို့၊ ဒီအကြောင်းတွေကို နားလည်သဘောပေါက်ပြီး ကိုယ့်ကိုယ်ကိုယ် ကာကွယ်ဖို့အတွက် ဆုံးဖြတ်ချက်တွေကို နေ့စဉ် ဘယ်လို ချမှတ်ရမလဲဆိုတာ သိရှိနိုင်စေဖို့နဲ့ ကိုယ်ကိုယ်တိုင်၊ ကိုယ့်မိသားစုနဲ့ တခြား အမျိုးသမီးတွေ အားလုံးအတွက် အင်တာနက်ကို လုံခြုံစိတ်ချရတဲ့ နေရာတစ်ခု ဖြစ်စေရေး ဘယ်လိုပါဝင်ကူညီနိုင်မလဲဆိုတာ သိရှိနိုင်စေဖို့ ဖြစ်ပါတယ်။

ပူးပေါင်းစီဉ်သည့် အဖွဲ့အစည်းများ

Internews

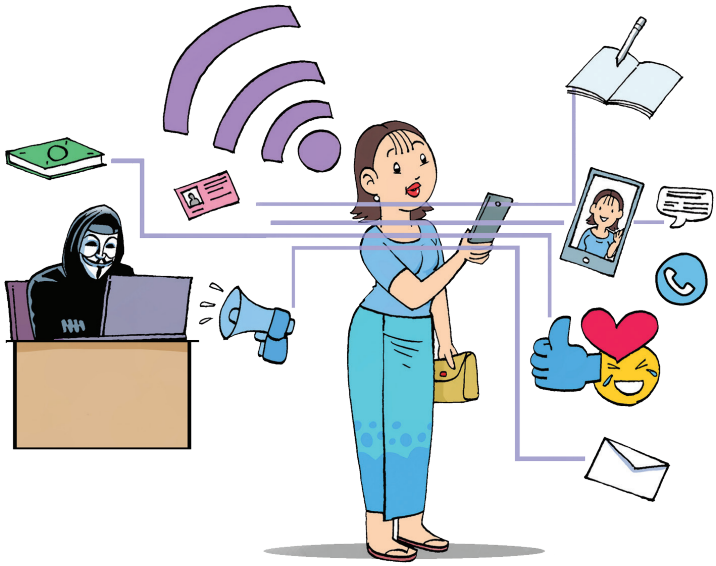
DEFENDERSTECH
A Project of DefendDefenders

Graphic design and research by POLLICY

မြန်မာဘာသာဖြင့် ပြန်လည်ထုတ်ဝေသည့် 'လုံခြုံဘဝ ညီအစ်မ' စာအုပ်ဖြစ်မြောက်ရေးအတွက် USAID၊ Civil Society and Media Project II (CSM II) အရပ်ဘက်အဖွဲ့အစည်းနှင့် မီဒီယာစီမံကိန်း-၂ တို့မှ ပံ့ပိုးကူညီခြင်းဖြစ်သည်။

ကျွန်မတို့ကဘယ်သူလဲ

ဒီစာအုပ်ပါ အကြောင်းအရာ၊ အချက်အလက်များကို Internews၊ အရှေ့နဲ့အရှေ့မြောက်အာဖရိကကျွန်းဆွယ်ရဲ့လူ့အခွင့်အရေးကာကွယ်ရေး စီမံကိန်းဖြစ်တဲ့ Defend Defenders နဲ့ ၂၀၁၇-၂၀၁၈ ခုနှစ် Safe Sister ပညာသင်အစီအစဉ်တို့က ပူးပေါင်းစီစဉ်ထားတာဖြစ်ပါတယ်။ ကျွန်မတို့ရဲ့ ရည်မှန်းချက်ကတော့ ဒီဂျစ်တယ်လုံခြုံရေးအကြောင်း ပိုပြီး ရှင်းရှင်းလင်းလင်း လွယ်လွယ်ကူကူနားလည် သဘောပေါက်စေဖို့၊ လက်တွေ့အသုံးပြုနေသူတွေ ပိုပြီး အံဝင်ခွင်ကျရှိစေဖို့နဲ့ အမျိုးသမီးနဲ့ မိန်းကလေးငယ်တွေအားလုံး အွန်လိုင်းလုံခြုံရေးနဲ့ ပတ်



သက်ပြီး မိမိဘာသာမိမိ ကာကွယ်ဖြေရှင်းနိုင်စေရေး တိုက်တွန်းအားပေးဖို့ ဖြစ်ပါတယ်။ အွန်လိုင်းမှာ ကိုယ့်ကိုယ်ကိုယ်ကာကွယ်ဖို့အတွက် အထိရောက်ဆုံးနည်းလမ်းတွေဟာ နေ့စဉ် အော့ဖ်လိုင်း(Offline)မှာ သုံးနေခဲ့ပြီးသားဖြစ်တဲ့ လက်တွေ့ဘဝ အသိဉာဏ်ပေါ်မှာ အခြေခံတဲ့ နည်းလမ်းတွေပဲဖြစ်တယ်ဆိုတာ စာဖတ်သူတွေ သတိပြုမိအောင် ဒီစာအုပ်က အကူအညီပေးလိမ့်မယ်လို့ မျှော်လင့်ပါတယ်။

မူမူကို တွေ့ကြရအောင်

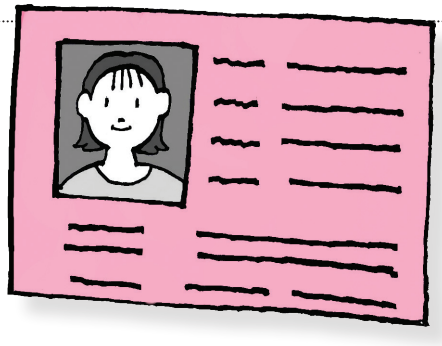
မူမူကတော့ မြန်မာနိုင်ငံ ရန်ကုန်မြို့မှ အမျိုးသမီးငယ်တစ်ဦးဖြစ်ပြီး သူနဲ့ သူ့သူငယ်ချင်းတွေအတွက် အင်တာနက်ဟာ ဘဝရဲ့တစ်စိတ်တပိုင်း ဖြစ်ပါတယ်။ Facebook မှာ သူတို့ ဒီနေ့ ဘာလုပ်ဖြစ်တယ်ဆိုတာ တင်ကြတယ်။ Instagram မှာ ဓာတ်ပုံတွေတင်ကြတယ်။ Twitter မှာလည်း တစ်ခါတလေ ဖလှယ်ကြတယ်။ WhatsApp နဲ့ Messenger မှာ သူငယ်ချင်းနဲ့ မိသားစုတွေဆီ စာတို့ (message) ပို့ကြတယ်။ Google မှာ သူတို့ သိချင်တာတွေ ရှာကြတယ်။ ပြီးတော့ အလုပ်အတွက် e-mail တွေ ပို့ကြတယ်။

မူမူမှာ နှင်းဆီလို့ခေါ်တဲ့ သမီးလေးတစ်ယောက်ရှိပါတယ်။ သူ့ရဲ့အမေ၊ အဖေနဲ့ ညီမငယ် ဖြူပြာတို့ဟာလည်း တစ်လမ်းတည်းသားချင်းတွေပါပဲ။ မူမူရဲ့ သူငယ်ချင်းတချို့ဟာ သူတို့ရဲ့ လူမှုမီဒီယာ Account တွေကို သူများတွေ ခိုးဝင်တာ ခံရပြီး သူတို့မသိဘဲ သူတို့ရဲ့ဓာတ်ပုံတွေ တင်တာကို ကြုံတွေ့ခဲ့ရဖူးပါတယ်။ ဒါကြောင့် မူမူ့အနေနဲ့ သူနဲ့ သူ့မိသားစုတို့ အွန်လိုင်းပေါ်မှာ ဘယ်လောက် လုံခြုံမှုရှိသလဲဆိုတာကို စိုးရိမ်ပူပန်နေပါတယ်။

ဒီစာအုပ်ငယ်မှာ မူမူက သူ့အနေနဲ့ အင်တာနက်သုံးတဲ့အခါ သူ့ရဲ့ အချက်အလက်တွေအပေါ် ဘာတွေဖြစ်နိုင်သလဲဆိုတာနဲ့ ပတ်သက်ပြီး မေးခွန်းတွေ မေးမှာဖြစ်သလို အွန်လိုင်းပေါ်မှာ သူ့အနေနဲ့ ပိုပြီး လုံခြုံမှုရှိစေဖို့ ဘယ်လိုနည်းလမ်းတွေ အသုံးပြုရမလဲဆိုတာနဲ့၊ သူ့သမီးနဲ့ သူငယ်ချင်းတွေကိုလည်း လုံခြုံမှုရှိစေဖို့ ဘယ်လိုသင်ကြားပေးရမလဲ ဆိုတာနဲ့ပတ်သက်ပြီး အကြံဉာဏ်တောင်းမှာ ဖြစ်ပါတယ်။

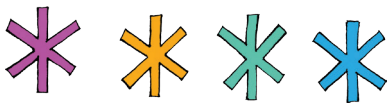
တစ်ယောက်ယောက်က ကျွန်မ account ထဲကို ခိုးဝင်လို့ရလားလို့ မူမူက မေးပါတယ်။

မူမူရဲ့ ညီအစ်မတဝမ်းကွဲဖြစ်တဲ့ အက်စ်သာဟာ ပြီးခဲ့တဲ့နှစ်တုန်းက သူ့ရဲ့ account ကို ခိုးဝင်တာ ခံရပြီး တစ်ယောက်ယောက်က အက်စ်သာ မရေး



တဲ့ဟာတွေကို အွန်လိုင်းပေါ် တင်လိုက်ပါတယ်။ အက်စ်သာက Facebook ကို ဆက်သွယ်ပြီး အကျိုးအကြောင်း ပြောပြပါတယ်။ နောက်ဆုံးမှာ အက်စ်သာဟာ သူ့ account ကို သူပြန်ရသွားခဲ့ပေမယ့် ဘာကြောင့် သူ့ account ခိုးဝင်ခံရတယ်ဆိုတာ ကိုတော့ အခုထိ မသိပါဘူး။

တစ်ယောက်ယောက်က အက်စ်သာရဲ့ account ထဲကို ဝင်နိုင်တဲ့ နည်းလမ်းတွေ အများကြီးရှိပါတယ်။ တစ်ယောက်ယောက်က သူရဲ့ Password (စကားဝှက်) ကို ခိုးသွားလို့လည်း ဖြစ်နိုင်ပါတယ်။ Password ခိုးတဲ့လူတွေ အများကြီးပဲ ရှိပါတယ်။ တကယ်တမ်းမှာ ဒီ Password ခိုးတဲ့ စီးပွားရေးလုပ်ငန်းက ကြီးထွားလာနေပါတယ်။ Password ခိုးတဲ့သူ Hacker တွေအတွက် သင့်ရဲ့ Password က အရေးပါတယ်။ ဘာလို့လဲဆိုတော့ အဲဒါက သင်နဲ့ပတ်သက်တဲ့ အချက်အလက်တွေကို ဖွင့်ဖောက်ရယူဖို့ သော့တစ်ချောင်းဖြစ်နေလို့ပါပဲ။ သူတို့ Password ခိုးတာ ဘာလို့ အောင်မြင်ကြသလဲ။



ဒါကို လုပ်ကြည့်ပါ။

- ခိုင်မာတဲ့ Password တစ်ခုဟာ Hacker တွေရဲ့ရန်က ကာကွယ်ဖို့ ပထမဆုံးအကာအကွယ်အဖြစ် ဆောင်ရွက်နိုင်ပါတယ်။ ဒါကြောင့် အမြော်အမြင်ရှိရှိ ရွေးချယ်ပါ။
- တကယ်လို့ Password တွေအားလုံးကို မှတ်မိဖို့ အခက်အခဲရှိတယ် ဆိုရင်တော့ Password Manager အပလီကေးရှင်း တစ်ခုခုကို စမ်းသုံးကြည့်ပါ။ သူက သင်ရဲ့ Password တွေအားလုံးကို သင့်အတွက် မှတ်ထားပေးမှာမို့ မာစတာ Password တစ်ခုကို မှတ်ထားဖို့ပဲလိုပါတယ်။

အကြောင်းတစ်ခုကတော့ ကျွန်မတို့သုံးတဲ့ Password ကို ကွန်ပျူတာက အလွယ်တကူ ဖြည်နိုင်၊ ဒါမှမဟုတ် ခိုးနိုင်ပြီးတော့ ဆိုက်ဘာရာဇဝတ်မှု ကျူးလွန်သူတွေက အသုံးပြုနိုင်လို့ပါပဲ။

အင်္ဂလိပ်မှာ အသုံးအများဆုံး Password တွေထဲက တစ်ခုဟာ p@ssw0rd ဆိုတာ သင်သိပါသလား။

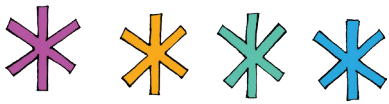
ပိုပြီးတော့ခိုင်မာတဲ့ Password တစ်ခုကို ဘယ်လိုဖန်တီးရမလဲလို့ မူမူက မေးပါတယ်။

အားထုတ်မှုကလေး နည်းနည်းလောက် လုပ်လိုက်ရုံနဲ့ သင့်ရဲ့ အွန်လိုင်း account တွေကို Hacker တွေရန်က ကာကွယ်ရာမှာ ကွာခြားမှု အကြီးကြီး ဖြစ်သွားနိုင်ပါတယ်။ သာမန် Password တွေဟာ တိုတောင်းပြီး ကွန်ပျူတာက လျင်လျင်မြန်မြန် ဖြည်နိုင်ဖို့ လွယ်ကူတာကြောင့်မို့ လုံလောက်မှုမရှိဘူးလို့ စိုးရိမ်ပူပန်မှုတွေ များလာနေပါတယ်။ အဲဒီအစား စကားစု စကားဝှက် (Passphrase) ကိုသုံးပါ။ Passphrase ဆိုတာကတော့ စကားလုံးတွေကို အုပ်စုတစ်ခုအဖြစ် စီစဉ်ထားတဲ့ Password တစ်မျိုးဖြစ်ပြီး ဖန်တီးသူအတွက် အဓိပ္ပာယ်တစ်စုံတစ်ရာရှိတဲ့ စကားစုပဲ ဖြစ်ပါတယ်။ Passphrase တွေဟာ မှတ်ရလွယ်ကူပြီးတော့ အဆင့်မြင့်ဆုံးဆိုတဲ့ ကွန်ပျူတာတွေကတောင် ဖြည်နိုင်ဖို့ ခက်ပါတယ်။

မူမူရဲ့ Facebook Password ကတော့ august2013! ဖြစ်ပြီး အဲဒါ က သူ့ညီမရဲ့ မွေးနှစ်နဲ့မွေးလ ဖြစ်ပါတယ်။ တော်တော်လေး ခန့်မှန်းဖို့လွယ်ကူတဲ့ Password ဖြစ်ပါတယ်။ ပိုပြီးခိုင်မာတဲ့ Passphrase ဖြစ်အောင်လို့ သူက အဲဒါကို EyeL1keMyFr1ends&Fam1ly လို့ ပြောင်းလိုက်ပါတယ်။ (သူ့အတွက် အဲဒါရဲ့အဓိပ္ပာယ်ကတော့ I like my friends and family. ငါ့ရဲ့ သူငယ်ချင်းတွေနဲ့ မိသားစုကို ငါချစ်တယ်လို့ အဓိပ္ပာယ်ရပါတယ်။)

ဒါကို လုပ်ကြည့်ပါ။

- ပိုရှည်လေပိုကောင်းလေပါပဲ။ သင့်ရဲ့ Password က စာလုံးရေ ၁၅ လုံးထက် ကျော်ပါစေ၊ ပြီးတော့ သင်္ကေတတွေ၊ ဂဏန်းတွေနဲ့ စာလုံးအကြီးတွေ ပါပါစေ။
- သင့်ရဲ့ Passphrase က အရမ်းကောင်းရင်တောင်မှ အမြဲတမ်းတော့ မလုံလောက်ပါဘူး။ သင့်ရဲ့ အရေးအကြီးဆုံး account တွေအတွက် ပိုပြီး လုံခြုံမှုလိုချင်တယ်ဆိုရင်တော့ အဆင့်နှစ်ဆင့်ပါ အတည်ပြုစနစ် (Two-Factor Authentication-2FA) ကို သုံးသင့်ပါတယ်။ (Facebook, G-mail, Twitter, Instagram) စတဲ့ လူသုံးအများဆုံး ဝက်ဘ်ဆိုက်ဒ်တွေမှာ သင့်ရဲ့ account တွေထဲကို ပိုမိုလုံခြုံစွာ Login ဝင်ရောက်နိုင်ဖို့အတွက် အဆင့်နှစ်ဆင့်ပါ အတည်ပြုစနစ်ကို ထောက်ပံ့ပေးထားပါတယ်။ ကြည့် ကြည့်လိုက်ပါ။
- Password ကို သုံးတာပဲဖြစ်ဖြစ် Passphrase ကို သုံးတာပဲဖြစ်ဖြစ် အဲဒါကို account တစ်ခုထက်ပိုပြီးတော့ မသုံးသင့်ပါဘူး။ ဘာဖြစ်လို့လဲဆိုတော့ တစ်ယောက်ယောက်က အဲဒီ Password ဒါမှမဟုတ် Passphrase ကို သိသွားမယ်ဆိုရင် သင့်ရဲ့ account တွေ အများကြီးထဲကို ဝင်သွားနိုင်လို့ပဲ ဖြစ်ပါတယ်။



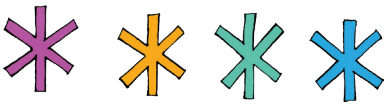
လူမှုမီဒီယာပေါ်မှာ ဘယ်လိုအကြောင်းအရာတွေကို တင်သင့်သလဲလို့ မူမူကမေးပါတယ်။

သင်ဟာ လူအများစုထဲက တစ်ယောက်ဆိုရင်တော့ လူမှုမီဒီယာဆိုတာ မိတ်ဆွေရှာဖို့နဲ့ မိသားစု၊ သူငယ်ချင်းတွေနဲ့ အဆက်အသွယ် မပြတ်စေဖို့ အဆင်ပြေတဲ့ နည်းလမ်းတစ်ခုပဲ

ဖြစ်ပါတယ်။ လူတွေက သူတို့နဲ့ပတ်သက်တဲ့ သတင်းအချက်အလက်တွေ အများကြီးကို ပို့စ်တင်ကြ၊ ပေးပို့ကြပါတယ်။ သူစိမ်းတွေက သူတို့ရဲ့ ဓာတ်ပုံတွေနဲ့ ကွန်းမန့် (Comment) တွေကို မြင်နိုင်ကြောင်း သူတို့ နောက်မှ သိကြပါတယ်။ သူစိမ်းတွေက သင့် Facebook Profile ကို ကြည့်တာနဲ့တင် သင့်အကြောင်း အများကြီးသိနိုင်ပါတယ်။

ဘယ်လို အကြောင်းအရာ စာတို (Message)၊ ဗီဒီယိုနဲ့ ဓာတ်ပုံတွေကို အွန်လိုင်းမှာတင်မလဲနဲ့ပတ်သက်ပြီး အမြော်အမြင်ရှိရှိ ရွေးချယ်ပါ။ ဘယ်လို ဓာတ်ပုံတွေကို ရိုက်သလဲနဲ့ သင့်ရဲ့ဘယ်လို အကြောင်းအရာ ကိုယ်ရေးကိုယ်တာ အချက်အလက်တွေကို ပို့သလဲဆိုတာနဲ့ ပတ်သက်ပြီး သတိထားပါ။

အွန်လိုင်းပေါ်တင်တဲ့ အရာမှန်သမျှ
လုံးဝပျောက်သွားတယ်ဆိုတာ မရှိဘူးဆိုတာကို သတိရပါ။

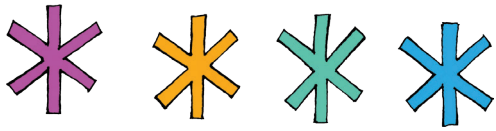


ဒါကို လုပ်ကြည့်ပါ။

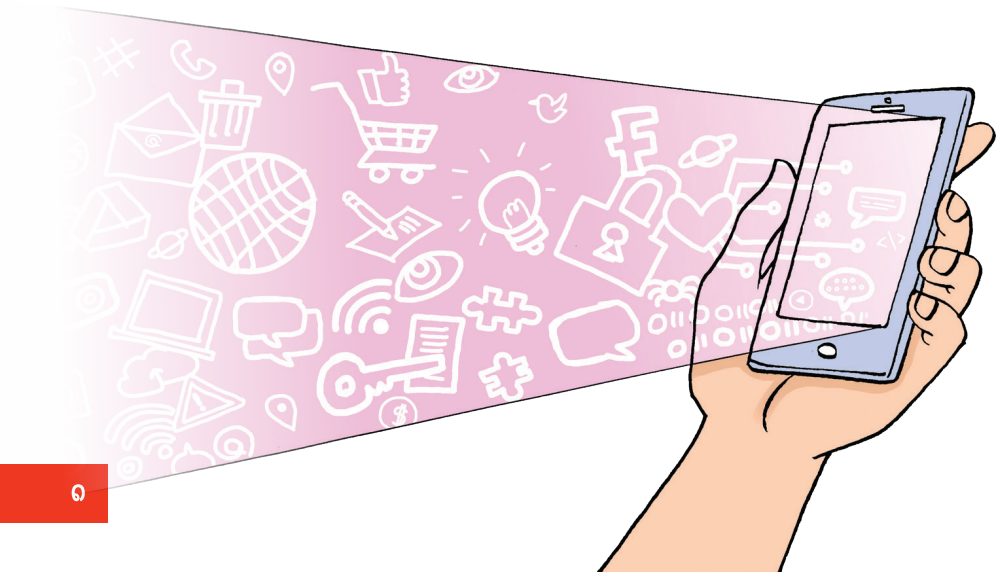
- သင့်ရဲ့နာမည်ကို Google မှာ ရိုက်ပြီးရှာကြည့်ပါ။ သင်နဲ့ပတ်သက်ပြီး အချက်အလက် ဘယ်လောက်များများ သူများတွေ ကြည့်လို့ရသလဲဆိုတာ စစ်ဆေးကြည့်ပါ။
- တကယ်လို့ သင့်ရဲ့ဖခင်က သင့်ရဲ့ လူမှုမီဒီယာစာမျက်နှာကို ကြည့်မယ်ဆိုရင် သင်နဲ့ပတ်သက်တဲ့ ကိုယ်ရေးကိုယ်တာ အချက်အလက် ဘယ်လောက်များများ သူတွေနိုင်မလဲ။ အဲဒီအချက်အလက်တွေကို သူသူငါငါ တွေနိုင်ကြတာနဲ့ပတ်သက်ပြီး သင်အဆင်ပြေရဲ့လား။ အဆင်မပြေဘူးဆိုရင် တော့ သင့်ရဲ့ account တွေရဲ့ Privacy Setting မှာ သင့်ရဲ့အချက်အလက်တွေကို ဘယ်သူတွေ မြင်နိုင်မလဲဆိုတာနဲ့ ပတ်သက်ပြီး ပြောင်းလိုက်ပါ။

Password မလိုဘဲနဲ့ တစ်ယောက်ယောက်က ကျွန်မ account ထဲကို ခိုးဝင်နိုင်သလားလို့ မူမူကမေးပါတယ်။

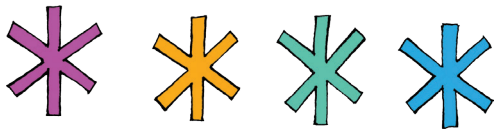
သင်မသိတဲ့ သူတွေဆီကနေ ရောက်တတ်ရာ ရာ Link တွေရဖူးပါသလား။ ဒါမဟုတ် သင် ဆုတစ်ခုခုရလို့ ဂုဏ်ယူပါတယ်ဆိုတဲ့စာမျိုး ရဖူးပါသလား။ ဒါမှမဟုတ် သင့်ကွန်ပျူတာမှာ ဗိုင်းရပ်စ်တွေရှိနေပြီ၊ အခုပဲ Update တစ်ခုကို Download လုပ်ဖို့လိုတယ်ဆိုတဲ့ အကြောင်းကြားစာမျိုးကို ရဖူးပါသလား။



သင့်ရဲ့ Password ကို ဖြည်တာအပြင် တစ်ယောက်ယောက်က သင့်ခွင့်ပြုချက်မရဘဲ သင့် account ထဲ ဝင်ရောက်နိုင်တဲ့ အခြားနည်းလမ်းတစ်ခုကတော့



သင့်ထံဗိုင်းရပ်စ် (Malware ဟုလည်းခေါ် သည်) ပို့လိုက်တာပါပဲ။ ဒီဗိုင်းရပ်စ်တွေကတော့ သင်ဘယ်သူဘယ်ဝါလဲဆိုတာနဲ့ သင့်ရဲ့ ငွေရေးကြေးရေးဆိုင်ရာ အချက်အလက်တွေအပါအဝင် အချက်အလက်တွေကို သင့်ရဲ့ကွန်ပျူတာ ဒါမှမဟုတ် account တွေကနေ ခိုးယူနိုင်တဲ့ အန္တရာယ်ရှိတဲ့ ကွန်ပျူတာပရိုဂရမ်တွေပဲ ဖြစ်ပါတယ်။ သင်က Link တစ်ခုခုကို နှိပ်လိုက်တဲ့အခါ ဒါမှမဟုတ် Malware ပါတဲ့ မယုံကြည်ရတဲ့ ဖိုင်တစ်ခုကို Download ဆွဲလိုက်တဲ့အခါမှာ သူတို့ သက်ဝင်လုပ်ဆောင်ပါတော့တယ်။



ဒါကို လုပ်ကြည့်ပါ။

- သတိထားပါ။ သင်မသိတဲ့သူတွေကနေပို့တဲ့ အီးမေးလ်ဖိုင်တွဲတွေ၊ Link တွေကို ဂရုပြုပါ။ ပို့တဲ့သူရဲ့ အချက်အလက်ကို သေသေချာချာ ကြည့်ပါ။ အဲဒါက ပုံမှန်ဟုတ်တဲ့ပုံမပေါ်ရင် အဲဒါကို မနှိပ်ပါနဲ့။

- သင့်ရဲ့ဖုန်း၊ ဒါမှမဟုတ် ကွန်ပျူတာမှာ ဗိုင်းရပ်စ်တွေရှိနေပြီ၊ Update တစ်ခုကို Download လုပ်ဖို့လိုတယ်လို့ အကြောင်းကြားစာ ရောက်လာတယ်ဆိုရင် သတိပြုပါ။ အဲဒါ အစစ်ဟုတ်ချင်မှ ဟုတ်ပါလိမ့်မယ်။ အဲဒါ အစစ်ဖြစ်တဲ့ပုံပေါ်ရဲ့လား သေသေချာချာကြည့်ပါ။ တကယ်လို့ မသေချာဘူးဆိုရင် Google ကို အသိပေးစာတို့ (Alert Message) ပို့ပြီး အခြားတစ်ယောက်ယောက်က report လုပ်ခဲ့သလားကြည့်ပါ။

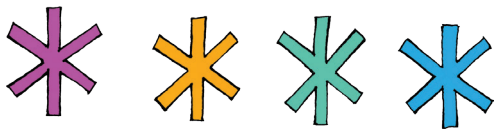
- သင့်ရဲ့ Software ကို Update လုပ်ဖို့ အကြောင်းကြားစာတွေကို လျစ်လျူမရှုပါနဲ့။ သင့်ရဲ့ Software Update တွေမှာ လုပ်ဆောင်ချက်အသစ်တွေနဲ့အတူ သင့်ကွန်ပျူတာကို ဗိုင်းရပ်စ်တွေကနေ ကာကွယ်ပေးတဲ့ လုံခြုံရေးအစီအမံအသစ်တွေ ပါဝင်တာကြောင့် Software တွေကို Update လုပ်ဖို့ အရေးကြီးပါတယ်။ သင့်အနေနဲ့ စိုးရိမ်ရင်တော့ Software ရဲ့ဝက်ဆိုက်ဒ်ကို သွားပြီး အဲဒီကနေ တိုက်ရိုက် Download ဆွဲယူနိုင်ပါတယ်။

ကျွန်မ အွန်လိုင်းမှာလုပ်တာတွေကို တစ်ယောက်ယောက်က စောင့်ကြည့်နေမလားလို့ မူမူကမေးပါတယ်။

အွန်လိုင်းမှာ စောင့်ကြည့်ခံနေရတယ်လို့ ခံစားမိတာက အများစုဖြစ်နေကျပါပဲ။ ဒါပေမဲ့ ဒါက တစ်ယောက်ယောက်က သင့်ကို ဗီဒီယိုရိုက်ပြီး တစ်ချိန်လုံး စောင့်ကြည့်နေတယ်လို့တော့ မဆိုလိုပါဘူး။ များသောအားဖြင့် သင် အင်တာနက် အသုံးပြုတဲ့အခါမှာ ဒီဂျစ်တယ်ခြေရာတွေ ကျန်ခဲ့ပါတယ်။ ဆိုလိုတာက ကျွန်မတို့ရဲ့ ဖုန်းတွေနဲ့ အချက်အလက်ဝင်ရှာတဲ့နေရာတွေ၊ ကျွန်မတို့ ဝင်ကြည့်တဲ့ ဝက်ဘ်ဆိုက်တွေ၊ ကျွန်မတို့အသုံးပြုတဲ့ အပလီကေးရှင်းတွေကို ခြေရာခံလို့ရပါတယ်။ ကျွန်မတို့ ကြိုက်

တဲ့အရာတွေ၊ သူငယ်ချင်းတွေနဲ့ မိသားစုဝင်ရဲ့နာမည်တွေ၊ ဘယ်ကျောင်းကို တက်ခဲ့သလဲဆိုတာတွေ၊ သင့်ရဲ့ နိုင်ငံရေးအမြင်တွေနဲ့ တစ်ခါတစ်ရံမှာ ပြီးခဲ့တဲ့ အပတ်က သင်ညစာ ဘာနဲ့စားခဲ့သလဲ ဆိုတာကိုတောင်မှ သိနိုင်ပါတယ်။

ကျွန်မတို့ နေ့စဉ်သုံးစွဲနေတဲ့ အဓိကဝက်ဘ်ဆိုက်တွေကို စီးပွားရေးလုပ်ငန်းတွေက ပိုင်ပြီးတော့ ကျွန်မတို့နဲ့ပတ်သက်တဲ့ အချက်အလက်တွေကို စုဆောင်းပြီး ကြော်ငြာသူတွေထံ ရောင်းခြင်းအားဖြင့် ပိုက်ဆံရှာပါတယ်။ အခု လော လောဆယ်တင်မှာပဲ အဲဒီကုမ္ပဏီတွေက သင့်ရဲ့ ဒီဂျစ်တယ် ခြေရာတွေကို စုဆောင်းကောင်း စုဆောင်းနေမယ့် ဖြစ်နိုင်ခြေ အများကြီးရှိပါတယ်။ ဒါပေမဲ့ သင့်ရဲ့ အချက်အလက်တွေ အများကြီး အွန်လိုင်းမှာ မကျန်ရစ်ရအောင် လျှော့ချနိုင်မဲ့နည်းလမ်းတွေ ရှိပါတယ်။



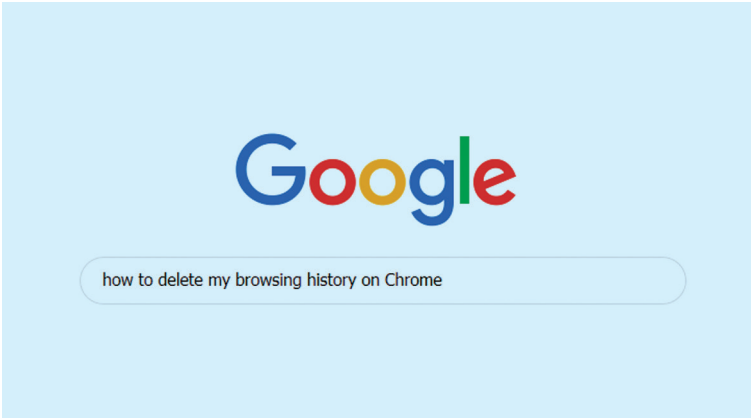
ဒါကို လုပ်ကြည့်ပါ။

- အပလီကေးရှင်းတစ်ခုကို အလကား အသုံးပြုနိုင်တယ်ဆိုရင် အဲဒီ အပလီကေးရှင်းကို ဖန်တီးတဲ့သူက အဲဒီ အပလီကေးရှင်းကနေ ပိုက်ဆံဘယ်လိုရသလဲ။ များသောအားဖြင့် အပလီကေးရှင်းကို အသုံးပြုတဲ့သူရဲ့ အချက်အလက်တွေကို ရယူပြီး ကြော်ငြာသူဆီ ရောင်းခြင်းအားဖြင့် ပိုက်ဆံရပါတယ်။
- သင်အသုံးပြုနေတဲ့ လူမှုမီဒီယာအားလုံးရဲ့ Privacy Setting ကို ပြန်စစ်ဆေးကြည့်ပါ။ သူတို့တွေက အချိန်တိုင်း ပြောင်းနေပါတယ်။
- သင့်ရဲ့ဖုန်းပေါ်မှာ App Permission ကို ဝင်ကြည့်ပြီး အပလီကေးရှင်းတွေက ဘယ်အရာတွေကို ဝင်ကြည့်လို့ရနေသလဲ ဆိုတာကို ကြည့်ကြည့်ပါ။ သင့်ရဲ့ အဆက်အသွယ်စာရင်း (Contact List)၊ မိုက်ခရိုဖုန်း၊ သင့်ရဲ့ တည်နေရာ စတာတွေကို ဝင်ကြည့်နိုင်တဲ့ အပလီကေးရှင်းတွေကို ဂရုပြုပါ။ လိုအပ်ရင် App Permission မှာ ပြောင်းပါ။

အခြားသူတွေနဲ့ ဖုန်း၊ ကွန်ပျူတာတွေကို အတူတကွသုံးစွဲရင် ဘယ်လိုလုပ်ရမလဲလို့ မူမူကမေးပါတယ်။

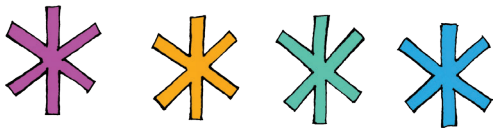
တကယ်လို့ သင်က အလုပ်မှာ၊ အိမ်မှာ ဒါမှမဟုတ် အင်တာနက်ကဖေးမှာ ကွန်ပျူတာတစ်လုံးကို အများနဲ့ မျှဝေသုံးစွဲမယ်ဆိုရင် အဲဒီ ကွန်ပျူတာကို အသုံးပြုတဲ့ အခြားသူတွေအနေနဲ့ သင်ဝင်ရောက်ကြည့်ရှုခဲ့တဲ့ ဝက်ဘ်ဆိုဒ်တွေ၊ သင့်ရဲ့ကိုယ်ရေးကိုယ်တာ Message တွေနဲ့ အီးမေးလ်တွေ၊ သင့်ရဲ့ ဓာတ်ပုံတွေ အပါအဝင် ကွန်ပျူတာပေါ်မှာရှိသမျှ သင့်ရဲ့အကြောင်းတွေကို လွယ်လွယ်ကူကူနဲ့ ကြည့်ရှုနိုင်တဲ့အပြင် သင့်ရဲ့ account ထဲဝင်ပြီး ဗီဒီယိုတွေ၊ စာတွေကိုတောင် တင်နိုင်ပါတယ်။

သင့်အကြောင်းအရာတွေကို တခြားသူတွေ မတွေ့နိုင်အောင်လုပ်ဖို့ အကောင်းဆုံးနည်းလမ်းကတော့ ကွန်ပျူတာကို အသုံးပြုပြီးနောက် မထွက်ခွာမီမှာ သင် ဘယ်ဝက်ဘ်ဆိုဒ်တွေကို ဝင်ရောက်ကြည့်ရှုခဲ့သလဲဆိုတဲ့မှတ်တမ်း (Browser History) ကို ဖျက်ပစ်ဖို့၊ (အီးမေးလ်နဲ့ လူမှုမီဒီယာကဲ့သို့သော) account တွေ အားလုံးကနေထွက် (Sign Out) လုပ်ဖို့နဲ့ ဖြစ်နိုင်ရင် အခုသုံးနေတဲ့ ကွန်ပျူတာ



ဆက်ရှင်ကနေထွက် (Log out) လုပ်ဖို့ပဲ ဖြစ်ပါတယ်။ တကယ်လို့ သင်က သင့်ရဲ့ ကိုယ်ရေးကိုယ်တာ စာရွက်စာတမ်းတွေ၊ ဓာတ်ပုံတွေကို သူများတွေမြင်မှာ စိုးရိမ်ရင်တော့ ကွန်ပျူတာပေါ်ကို Download မဆွဲပါနဲ့။ အဲဒီအစား Google Drive ဒါမှမဟုတ် Dropbox လို Cloud တွေထဲ ထည့်သိမ်းပါ။ ဒါပေမဲ့ ဘယ်လိုပဲဖြစ်ဖြစ် ကွန်ပျူတာကနေခွာတော့မယ်ဆိုရင် Sign out လုပ်ဖို့ မမေ့ပါနဲ့။

သင့်ရဲ့ကွန်ပျူတာ ဒါမှမဟုတ် ဖုန်းကို မိသားစုဝင်တွေနဲ့ပဲ အတူသုံးတယ်ဆိုရင် တောင်မှ သူတို့ကို အသိပေးပြီး Password ဒါမှမဟုတ် Number Lock (တစ်ခါတစ်ရံ ပင်နံပါတ်ဟုလည်းခေါ်) ထားဖို့ အရေးကြီးပါတယ်။ ဒါမှသာ သင့်ရဲ့ကွန်ပျူတာ ဒါမှမဟုတ် ဖုန်းအခိုးခံရတဲ့ အခြေအနေမျိုးမှာ သင့်အတွက် အရေးကြီးတဲ့ အချက်အလက်တွေနဲ့ ဓာတ်ပုံတွေကို ခိုးသွားတဲ့သူက ဝင်မကြည့်နိုင်မှာ ဖြစ်ပါတယ်။



ဒါကို လုပ်ကြည့်ပါ။

- တကယ်လို့ သင်မယုံကြည်ရတဲ့သူ တစ်ယောက်ယောက်နဲ့ ကွန်ပျူတာကို မျှဝေသုံးမိတယ်ဆိုရင် သူတို့က သင်ဘာလုပ်သလဲ ဆိုတာ ခြေရာခံနိုင်တဲ့ Software တစ်ခုခုကို ထည့်သွင်းကောင်း ထည့်သွင်းနိုင်ပါတယ်။ ဒီ Software ကို Spyware လို့ ခေါ်လေ့ရှိကြပါတယ်။ တကယ်လို့ Spyware ထည့်သွင်းထားတဲ့ ကွန်ပျူတာတစ်ခုကို သုံးနေရတယ်လို့ သံသယရှိရင် အဲဒီကွန်ပျူတာပေါ်မှာ သင့်ရဲ့ လုပ်ဆောင်မှုတွေနဲ့ ပတ်သက်ပြီး သတိထားဖို့လိုပါတယ်။
- တကယ်လို့ သင်သိတဲ့ တစ်ယောက်ယောက်က သင့်ရဲ့ ကိုယ်ရေးကိုယ်တာ Message တွေကို ဖတ်ဖို့ သင့်ဖုန်းထဲ ဝင်ကြည့်မယ်ဆိုရင် သင့်အနေနဲ့ သူများမမြင်စေလိုတဲ့ message တွေကို ဖျက်ထားဖို့ လိုပါတယ်။

မူမူရဲ့လုပ်ရန်ဇယား

အခုဆိုရင် မူမူက သူ့ရဲ့ ဒီဂျစ်တယ်လုံခြုံရေးကို ပိုပြီးကောင်းမွန်အောင်လုပ်ဖို့ စိတ်ဝင်စားသွားပြီဆိုတော့ သူဘာတွေလုပ်မလဲ ကြည့်လိုက်ကြရအောင်။

1 **ပိုပြီးကောင်းတဲ့ Password တွေထားမယ်။**

ကိုယ့်အကြိုက်ဆုံး သီချင်းစာသားကို သင်္ကေတတွေ၊ ဂဏန်းတွေနဲ့ စာလုံးအကြီးတွေနဲ့ပေါင်းလို့ ခိုင်မာတဲ့ Passphrase တစ်ခုထားမယ်။ account တွေ အများကြီးအတွက် Password တစ်ခုတည်း မသုံးဘူး။

2 **ကလစ်ကို မနှိပ်ခင်မှာ စဉ်းစားမယ်။**

အခုကစလို့ သံသယဖြစ်ဖွယ် Link တွေနဲ့ ဖိုင်တွဲတွေကို ကလစ်မနှိပ်တော့ဘူး။ မသိတဲ့လူတွေဆီက အီးမေးလ် ဝင်လာရင် ပို့တဲ့သူရဲ့အချက်အလက်နဲ့ အီးမေးလ်ရဲ့အကြောင်းအရာကို သတိထားကြည့်ပြီး ဂရုစိုက်မယ်။

3 **အမြဲတမ်း Log out လုပ်မယ်။**

သင့်ရဲ့ဖုန်းနဲ့ကွန်ပျူတာပေါ်က လုံခြုံရေးဆက်တင်တွေကို ပြန်စစ်ကြည့်ပါ။ Password ထားပါ။ အတူတူမျှဝေသုံးတဲ့ ဖုန်း ဒါမှမဟုတ် ကွန်ပျူတာကနေ ထွက်ခွာတိုင်း ကိုယ့်ရဲ့ account တွေထဲကနေ Sign out လုပ်ပါ။

4 **ဘာတွေကို အွန်လိုင်းပေါ်တင်မလဲဆိုတာနဲ့ ပတ်သက်ပြီး ဂရုစိုက်ပါ။**

အင်တာနက်ပေါ်မှာ ပုံ၊ ဒါမှမဟုတ် စာတိုတင်လိုက်တာနဲ့ အဲဒါကို ပြန်ဖျက်ဖို့ဆိုတာ မဖြစ်နိုင်သလောက်ပါပဲ။ ဒါကြောင့် လူမှုမီဒီယာတွေမှာ တစ်ခုခုကိုမတင်မီ သေသေချာချာစဉ်းစားပါ။ လူမှုမီဒီယာ အပလီကေးရှင်းတွေနဲ့ ဝက်ဘ်ဆိုဒ်တွေမှာ သင့်ရဲ့ Privacy Setting တွေကို ပြန်စစ်ကြည့်ပါ။ (တည်နေရာ၊ မိုက်ခရိုဖုန်း၊ အဆက်အသွယ်) တွေကို အပလီကေးရှင်းတွေက ဝင်ရောက်ကြည့်ရှုနိုင်မှုကို ကန့်သတ်ပါ။ သင်တင်ထားတွေကို မြင်နိုင်တဲ့သူတွေကိုလည်း ကန့်သတ်ပါ။

5 **သင့်ရဲ့ညီအစ်မတွေကို စောင့်ရှောက်ပေးတဲ့သူဖြစ်ပါစေ။**

အွန်လိုင်းပေါ်မှာ ပေါက်ကြားသွားတဲ့ ဓာတ်ပုံတွေဟာ အမျိုးသမီးတွေ အများကြီးကို နာကျင်ခံစားရစေပါတယ်။ ကိုယ့်လိုပဲ အမျိုးသမီးတွေကို ညီအစ်မတွေလို ဂရုစိုက်တဲ့အနေနဲ့ မသင့်တော်တဲ့ အကြောင်းအရာတွေကို အွန်လိုင်းပေါ်မှာ Forward မလုပ်ပါနဲ့။ အမျိုးသမီးတွေကို အွန်လိုင်းအနိုင်ကျင့်ဖို့နဲ့ အကြမ်းဖက်ဖို့ သူတို့ရဲ့ account တွေကို ပလက်ဖောင်းအဖြစ် အသုံးပြုသူတွေကို သူငယ်ချင်းစာရင်းကနေ ဖယ်ထုတ်ပါ။ report လုပ်ပါ။

သတိရပါ။ သင်လုပ်နိုင်ပါတယ်။

အွန်လိုင်းပေါ်မှာ လုံခြုံမှုရှိတယ်ဆိုတာ ဘာလဲဆိုတာ သင်ယူဖို့ အချိန်ပေးပါ။ အင်တာနက်အသုံးပြုတဲ့အခါ သတိထားပါ။ သင့်ရဲ့အကောင်းဆုံးအရည်အချင်းကတော့ မူမမှန်တဲ့အရာတွေကို သတိပြုနိုင်စွမ်းနဲ့ တခြားသူတွေဆီကို မပျံ့နှံ့သွားမှီ ပြဿနာတွေကို ဖော်ထုတ်နိုင်စွမ်းပဲ ဖြစ်ပါလိမ့်မယ်။