ဒစ်ဂျစ်တယ်လုံခြုံမှုလက်စွဲ

စာနယ်ဇင်းသတင်းသမားများသည် ၎င်းတို့ကိုယ်တိုင်နှင့် ၎င်းတို့၏ အဆက်အသွယ်အရင်းအမြစ်များ ကို ခြိမ်းခြောက်အန္တရာယ်ပေးခြင်းမှ ကာကွယ်ထားနိုင်ရန်အတွက် Hacking (တစ်ပါးသူ၏ကွန်ပျူတာမှ အချက်အလက်များကို ရယူနှောက်ယှက်ခြင်း)၊ Phishing (အစစ်ကဲ့သို့ဟန်ဆောင်၍ မသမာမှုပြုလုပ်ခြင်း) နှင့် Surveillance (စောင့်ကြည့်ခြင်း) စသည်တို့နှင့်ပတ်သက်သည့် နောက်ဆုံးပေါ် ဒီဂျစ်တယ်လုံခြုံရေးဆိုင်ရာ သတင်းများကို အချိန်နှင့်တပြေးညီ အမြဲတမ်းရယူနေရမည်။ စာနယ်ဇင်းသတင်းသမားများသည် မိမိတာဝန် ခံရသည့် သတင်းအချက်အလက်များကို ကာကွယ်ရမည်ဟုမှတ်ယူကာ မှားယွင်းသောသူများလက်တွင်းသို့ မရောက်ရှိစေရန်အတွက် မိမိ၏ အကောင့်များ၊ ပစ္စည်းကိရိယာများ၊ ဆက်သွယ်ရေးနှင့် အွန်လိုင်းသုံးစွဲမှုများကို အကာအကွယ်ပြုလုပ်ထားသင့်သည်။

မာတိကာ

(၁) သင့်အကောင့်များကို ကာကွယ်ပါ (Protect Your Accounts)

သင်၏အကောင့်များကိုကာကွယ်ရန် -

စာနယ်ဇင်းသတင်းသမားများသည် အွန်လိုင်းအကောင့်အမျိုးမျိုးကို အသုံးပြုလေ့ရှိကြပြီး၊ ၎င်းနှင့် ၎င်းတို့၏ လုပ်ဖော်ကိုင်ဖက်များ၊ မိသားစုများနှင့် သတင်းရင်းမြစ်အဆက်အသွယ်များ(Sources) စသည်တို့ကို ၎င်းတို့၏ ကိုယ်ရေးကိုယ်တာနှင့် အလုပ်နှင့်ဆိုင်သောအကောင့်များတွင်ပါ သိမ်းထားလေ့ရှိကြသည်။ အကောင့်များကို လုံခြုံစွာသိမ်းဆည်းထားခြင်း၊ သတင်းအချက်အလက်များကို ပုံမှန်အရန်သိမ်းခြင်းနှင့် ဖယ်ရှားခြင်းတို့က ဟက်ကာများ၏ ရန်ကိုကာကွယ်နိုင်သည်။ ခေတ်မီနည်းပညာစွမ်းရည်ရှိသော ဆန့်ကျင်ဘက်၏ ပစ်မှတ်ထားခံရမည့် စာနယ်ဇင်းသတင်းသမားများအတွက် ဤအဆင့်များကိုဆောင်ရွက်ရန် အထူးအရေးကြီးသည်။

- အကောင့်တစ်ခုစီတွင် မည်သည့်သတင်းအချက်အလက်များကို သိမ်းဆည်းထားသည်ကို သိရှိထားပါ။ သင်၏အကောင့်ကို ချိုးဖောက်ခံရပါက သင်၊ သင်၏ မိသားစုနှင့်

သင့်အဆက်အသွယ်များအပေါ်တွင် သက်ရောက်လာနိုင်မည့် အကျိုးဆက်များကိုလည်း စဉ်းစားပါ။

- မိမိ၏ ကိုယ်ပိုင်ကိစ္စအပြင်အဆင် (Privacy Settings) များကို ပြန်လည်စစ်ဆေးပါ။ အထူးသဖြင့် လူမှုမီဒီယာတွင် မည်သည့်သတင်းအချက်အလက်များကို လူအများသိစေရန် ဖေါ်ပြထားသည်ကို သိမြင်နားလည်နေပါ။
- အကဲဆတ်သော သတင်းအချက်အလက်များ သို့မဟုတ် ပုဂ္ဂိုလ်ရေးဆက်သွယ်စာများအပါအဝင် အများပြည်သူသို့ မသိစေလိုသော သတင်းအချက်အလက်များစသည့် မည်သည့်အချက်အလက်များကို မဆို မိတ္တူမူပွားဖြင့်အရန်သိမ်းဆည်းခြင်း (Backup Copies) လုပ်ထားပါ။ ပြီးလျှင် ၎င်းတို့အားလုံးကို သင့်အကောင့် သို့မဟုတ် Device ထဲမှ ပယ်ဖျက်ပါ။ ၎င်းမိတ္တူမူပွားများကို ပြင်ပExternal Drive တစ်ခု သို့မဟုတ် **အဝေးရှိသိမ်းဆည်းရာနေရာ** (Cloud) တွင် လုံခြုံစွာသိမ်းဆည်းထားပါ။
- သင်အသုံးမပြုတော့သော မည်သည့်အကောင့်များကိုမဆို ဖျက်ပစ်ပါ။ သင်သိမ်းဆည်းလိုသည့် မည်သည့်သတင်းအချက်အလက်ကိုမဆို မိတ္တူမူပွားများကူးထားရန် သတိရပါ။
- အကောင့်တိုင်းအတွက် ထူးခြားသော စကားဝှက် (Password) များကို ဖန်တီးအသုံးပြုပါ။ စကားဝှက် (Password) များကို ပြန်၍မသုံးပါနှင့်။ သင်၏ စကားဝှက်များကို စီမံနိုင်ရန် စကားဝှက်မန်နေဂျာကို အသုံးပြုပါ။
- အစစ်အမှန်ဖြစ်ကြောင်း နှစ်ဘက်စလုံးကိုအပြန်အလှန်အသိအမှတ်ပြုခြင်း (Two-Factor Authentication - 2FA) ကိုဖွင့်ပြီး၊ ဖြစ်နိုင်လျှင် Yubikey ကဲ့သို့သော (နှစ်ဆင့်ခံဖွင့်ရသော) လုံခြုံရေး သော့ (Key) ကိုသုံးပါ။
- အကောင့်တစ်ခုစီ၏ အကောင့်အသုံးပြုမှု (Account Activity) အပိုင်းကို ပုံမှန်ပြန်လည်စစ်ဆေးပါ။
  ဤကဲ့သို့ပြုလုပ်ခြင်းဖြင့် Device များတွင် သင်အသိအမှတ်မပြုပဲ တစ်စုံတစ်ဦးက ဖွင့်လှစ်ဝင်ရောက် (Logged in) ခဲ့ကြောင်း သိရှိလိမ့်မည်။

(၂) **အစစ်ကဲ့သို့ဟန်ဆောင်၍ မသမာမှုပြုလုပ်ခြင်း (Phishing)**

စာနယ်ဇင်းသတင်းသမားများသည် မိမိသည်မည်သူဖြစ်ကြောင်း (Profile) ကို အများပြည်သူများက သိရှိနေသောကြောင့်၊ ၎င်းတို့၏ အဆက်အသွယ်အချက်အလက်များသည် မျက်စေ့ကျစရာဖြစ်တတ်ကြသည်။

စာနယ်ဇင်းသတင်းသမားများ၏ Data နှင့် Devices များကို ဝင်ရောက်ရှာဖွေလိုသော ရန်သူများသည် အစစ်ကဲ့သို့ဟန်ဆောင်၍ ဖန်တီးထားသော အီးမေးလ်၊ တယ်လီဖုန်းမက်ဆေ့ချ် (SMS)၊ လူမှုရေးမီဒီယာ (Social Media) များမှတစ်ဆင့် သို့မဟုတ် လက်ခံသူ၏ အရေးကြီးအချက်အလက်များကို ရယူနိုင်သည့်

စကားပြောမက်ဆေ့ချ် (Chat) များမှတစ်ဆင့် လှည့်စားဝင်ရောက်ခြင်း (Trick) ဖြင့်လည်းကောင်း၊ လင့်ခ်တစ်ခုကိုနှိပ်ခြင်း သို့မဟုတ် ဖိုင်တစ်ခုကို ဒေါင်းလုပ်ပြုလုပ်ခြင်းအားဖြင့် အဆင့်မြင့်နည်းပညာ အသုံးပြုထားသည့် အန္တရယ်ပေးနိုင်သော၊ ဒုက္ခပေးနိုင်သော ဆော့ဖ်ဝဲလ် (Malware) နှင့် သူလျှိုဆော့ဖ်ဝဲလ် (Spyware) များမှတစ်ဆင့်လည်းကောင်း အဆိုပါ Devices များထဲရှိ အရေးကြီးအချက်အလက်များကို ရယူ နိုင်သည်။ အဆင့်မြင့်နည်းပညာသုံး ရွပ်ထွေးသည့် Malware နှင့် Spyware အမျိုးအစားများစွာရှိရာတွင် အဆင့်အမြင့်ဆုံး ဆော့ဖ်ဝဲလ်များသည် အဝေးမှနေ၍ အဆိုပါ Devices များနှင့် ၎င်းထဲရှိ အချက်အလက်များ အတွင်းသို့ ဝင်ရောက်ပြီး အချက်အလက်များကိုရယူနိုင်သည်။

Phishing တိုက်ခိုက်မှုများမှ ကာကွယ်ရန် -

- သင်နှင့် သင်သိသူတစ်ဦးဦးက ပစ်မှတ်ဖြစ်နိုင်ကြောင်း ခြိမ်းခြောက်မှုနှင့် ခြိမ်းခြောက်ခံရနိုင်ချေရှိမှုကို နားလည်ရန် ရန်သူများ၏ နည်းပညာစွမ်းရည်များကို လေ့လာထားပါ။
- မြန်မြန်လုပ်ရန်တိုက်တွန်းခြင်း သို့မဟုတ် အလွန်မှန်ကန်သည်ဟုထင်ရသော အရာတစ်ခုခုကို ပြုလုပ်ရန် တိုက်တွန်းနေသည့် မက်ဆေ့ချ်များကို သတိထားပါ။ အထူးသဖြင့် ၎င်းတို့သည် လင့်ခ် (Link) တစ်ခုကို နှိပ်ဖွင့်စေခြင်း သို့မဟုတ် ပူးတွဲဖိုင်တစ်ခုကို ဒေါင်းလုပ်ပြုလုပ်စေခြင်းတို့ပါဝင်သည်။
- ပေးပို့သူ၏ အကောင့်နှင့်ပတ်သက်သော အသေးစိတ်အချက်အလက်များနှင့် မက်ဆေ့ချ်တွင်ပါဝင်သော အကြောင်းအရာများသည် အမှန်အကန် ဟုတ်၊ မဟုတ်ကို သေချာစွာစစ်ဆေးပါ။ စာလုံးပေါင်း၊ သဒ္ဒါ၊ အပြင်အဆင် သို့မဟုတ် အရေးအသားပုံစံဟန်ပန် စသည့် အသေးအဖွဲများကွဲပြားနေခြင်းသည် အကောင့်ကို Hacking သို့မဟုတ် Spoofed လုပ်ခြင်းခံနေရသည်ကို ပြသသည်။
- သံသယဖြစ်ဖွယ် သို့မဟုတ် မမျှော်လင့်သောဆက်သွယ်မှုဖြစ်ပါက ဖုန်းခေါ်ဆိုမှုကဲ့သို့သော အခြားနည်းလမ်းဖြင့် ပေးပို့သောသူနှင့် မက်ဆေ့ချ်ကိုအတည်ပြုပါ။
- မက်ဆေ့ချ်သည် သင်သိသူတစ်ဦးထံမှ ဖြစ်ပုံရသော်လည်း လင့်ခ်များကိုမနှိပ်ခင် သေချာစွာစဉ်းစားပါ။ သည်။ ဆက်သွယ်သူ၏ URL သည် တရားဝင်ပုံ ရှိ၊ မရှိ ကြည့်ရှုရန် လင့်ခ်များပေါ်တွင် သင်၏ Cursor ကို တင်ထားပါ။
- Malware ပါနိုင်သည့် ပူးတွဲပါဖိုင်ကို ဒေါင်းလုပ်မလုပ်မီစေရန် အီးမေးလ်ဖြင့်ပေးပို့လာခံရရှိသော ပူးတွဲပါဖိုင်များကို သုံးသပ်လေ့လာပါ။ သံသယဖြစ်ပါက ပေးပို့သူကိုခေါ်ဆို၍ အကြောင်းအရာကို အီးမေးလ်စာကိုယ်ထဲသို့ ကူးယူပြီး ပေးပို့ရန်တောင်းဆိုပါ။

- သံသယဖြစ်ဖွယ်ရှိသော လင့်ခ်များနှင့် စာရွက်စာတမ်းများကို ဖြစ်နိုင်ချေရှိသော Malware များ အတွက်စစ်ဆေးပေးသည့် **လူသိများသည့်** Virus Total ဆော့ဖ်ဝဲလ်သို့ တင်ပါ။ Virus Total ဆော့ဖ်ဝဲလ် သည် ဖြစ်နိုင်ချေရှိသော Malware များကိုသာ စစ်ဆေးပေးသည်။
- နောက်ဆုံးပေါ်နည်းပညာများကို အမြဲတစေအလိုအလျောက် Update ဖြစ်နေစေပြီး၊ သင်၏ Devices များပေါ်ရှိ ဆော့ဖ်ဝဲလ်များအား လုံးအတွက် နောက်ဆုံးပေါ်နည်းပညာများကို အမြဲရယူထားပါ။ ဤနည်းဖြင့် Malware ကြောင့် ဖြစ်နိုင်ခြေရှိသော သင်၏လုံခြုံရေးကိုအန္တရာယ်ပြုနိုင်သည့် အားနည်းချက်များကို ဖြေရှင်းနိုင်လိမ့်မည်။
- ရွေးကောက်ပွဲများနှင့် မငြိမ်သက်မှုကာလအတွင်း လုပ်ဖော်ကိုင်ဖက်များ သို့မဟုတ် ဒေသခံ အရပ်ဘက်လူ့အဖွဲ့အစည်းများကို ပစ်မှတ်ထားခံရနိုင်သည်ဟု သတိပေးခံရလျှင် Phishing ပြုလုပ်လာနိုင်ကြောင်းကို အထူးသတိထားပါ။

(၃) ပစ္စည်းကိရိယာလုံခြုံရေး (Device Security)

စာနယ်ဇင်းသတင်းသမားများသည် ပါဝင်သောအရာများကို လုပ်ဆောင်ရန်၊ သိမ်းဆည်းရန်နှင့် အဆက်အသွယ်ပြုလုပ်ရန်အတွက် Devices အမျိုးမျိုးကို အသုံးပြုကြသည်။
စာနယ်ဇင်းသတင်းသမားအများစု၊ အထူးသဖြင့် အလွတ်တန်းသတင်းသမားများသည် ၎င်းတို့၏ တူညီသော Devices များကို အိမ်တွင်လည်း အသုံးပြု၊ အလုပ်တွင်လည်း အသုံးပြုကြခြင်းတို့ကြောင့် ၎င်းတို့၏ Devices များ ပျောက်ဆုံးခြင်း၊ အခိုးခံရခြင်း သို့မဟုတ် သိမ်းဆည်းခံရခြင်းတို့ရှိပါက သတင်းအချက်အလက်အမြောက်အများကို ဖော်ထုတ်ခြင်း ခံရနိုင် သည်။ အထူးသဖြင့် ခရီးသွားလျှင် Encrypt ပြုလုပ်ထားသော ကွန်ပျူတာ Hard Drive များ၊ ဖုန်းများ၊ Tablets နှင့် External Storage Devices **များအတွင်းရှိအချက်အလက်များကို** အခြားသူများက Password မပါဘဲ ဝင်ရောက်ခြင်းမရှိနိုင်စေရန် သေချာမှုရှိပါစေ။

သင်၏ စက်ကိရိယာ (Device) များလုံခြုံစေရန် -

- Devices များကို စကားဝှက်၊ လျို့ဝှက်နံပါတ် (Code) သို့မဟုတ် လျို့ဝှက်ဂဏန်း (PIN) ဖြင့် သော့ခတ်(Lock)ပါ။ ရှည်လျားသော ကိုယ်ပိုင်သတ်မှတ်နံပါတ်များ သို့မဟုတ် စကားဝှက်များ ကို အသုံးပြုခြင်းဖြင့် အခြားသူများက သော့ဖွင့် (Unlock) ဝင်ရောက်နိုင်ရန် ခက်ခဲစေပါသည်။
- Devices များကို နောက်ဆုံးပေါ် Malware အန္တရာယ်များမှကာကွယ်ရန် သင့် Operating System ကို Update လုပ်ပါ။
- သင်၏ Devices များပေါ်တွင် သိမ်းဆည်းထားသော သတင်းအချက်အလက်များကို စစ်ဆေးပြီး၊ ၎င်းသည် သင်နှင့်အခြားသူများကို မည်သို့အန္တရာယ်ပေးနိုင်သည်ကို စဉ်းစားပါ။

- အကယ်၍ သင်၏ Devices များ ပျက်စီးခြင်း၊ ပျောက်ဆုံးခြင်း သို့မဟုတ် အခိုးခံရခြင်း ဖြစ်လျှင် သိမ်းဆည်းထားသော သတင်းအချက်အလက်များကို မဆုံးရှုံးစေရန် Devices များကို ပုံမှန် အရန်ကူးယူမှု (Backup) လုပ်ထားပါ။ ထိုအရန်ကူးထားသော အရန်ကူးယူမှု (Backup) မူပွားကို သင့်ပုံမှန်အလုပ်နေရာမှ ဝေးသောနေရာတွင်လုံခြုံစွာသိမ်းဆည်းပါ။
- Chat Message အပါအဝင် အကဲဆတ်သော သတင်းအချက်အလက်များကို ပုံမှန်ဖျက်သိမ်းနေပါ။ ပယ်ဖျက်ထားသော ဖိုင်များကို မိမိ၏ ဆန့်ကျင်ဘက်က ပြန်လည်ရယူနိုင်ခြင်းမှ ကာကွယ်ရန်အတွက် ဖြစ်နိုင်ပါက Device အတွင်းရှိ အချက်အလက်များကို လုံခြုံစိတ်ချစွာဖျက်သိမ်းနိုင်သည့် Software (Secure Deletion Software) ကို အသုံးပြုပြီးမှ ဖျက်သိမ်းပါ။ သို့မဟုတ်ပါက Reset လုပ်ပြီး၊ ဆက်စပ်မှုမရှိသော အခြားကိစ္စရပ်များအတွက်အသုံးပြုကာ စက်၏ မှတ်ဉာဏ် (Device Memory) ကို အသစ်ပြန်ဆွဲ(Rewrite) ပါ။ (ဤသို့မဆောင်ရွက်မီ မိမိသိမ်းထားလိုသောအရာများကို ကူးယူထားပါ။ သို့မဟုတ်ပါက သင့် သတင်းအချက်အလက်များအားလုံးကိုပါ ဆုံးရှုံးသွားလိမ့်မည်။)
- အများသုံးနေရာများတွင် မိမိအသုံးပြုနေသော Devices များကို အားသွင်းနေစဉ်ချိန် အပါအဝင် ကိုယ်တိုင်မရှိနေပဲ မထားခဲ့ပါနှင့်။ သို့မဟုတ်ပါက ပစ္စည်းများကို ခိုးယူခြင်း သို့မဟုတ် ဖျက်ဆီးခြင်း ခံရနိုင်သည်။
- မိမိအသုံးပြုနေသော Devices များကို အများသုံး USB အားသွင်းချိတ်ဆက်နေရာ USB Port သို့မဟုတ် အခမ်းအနားများတွင် အခမဲ့ဖြန့်ဝေပေးသော USB ပလပ်ပေါက်နေရာ (USB Flash Drives)များတွင် ထည့်သွင်းအသုံးမပြုပါနှင့်။ ၎င်းနေရာများ၌ Malware များပါရှိလာနိုင်သဖြင့် ၎င်းတို့မှတစ်ဆင့် သင့်ကွန်ပျူတာကို အန္တရာယ်ပေးနိုင်သည်။
- သင်၏ Devices များထဲရှိ အချက်အလက်များသည် ဖုန်းနှင့်ချိတ်ဆက်ထားသော Cloud Account များထဲ၌ အမြဲတမ်း အရန်သင့် Back up အနေနှင့်ရှိနေသည်ကို သတိပြုပါ။ Cloud ထဲတွင် သိမ်းဆည်းထားသော သတင်းအချက်အလက်များသည် Encrypted မလုပ်ထားပါ။ သင်၏ Setting များတွင် Automatic Back up ကို ပိတ်ထားနိုင်သည်။
- Devices များကို ခိုးယူခံရလျှင် သင်၏ Devices များမှ အချက်အလက်များကို အဝေးမှဖယ်ရှားရှင်းလင်း နိုင်အောင် Set up လုပ်ထားပါ။ ဤ Set up ကို ကြိုတင်ဆောင်ရွက်ရန်ဖြစ်သည်။ အင်တာနက်နှင့် ချိတ်ဆက်ထားသော Devices များမှသာလျှင် အဝေးမှနေ၍ ဖယ်ရှားရှင်းလင်းခြင်းကို ပြုလုပ်နိုင်သည်။
- မိမိ၏ Devices များကို စိတ်ချရသောဝန်ဆောင်မှုပေးသူ (Reputable Dealer)များထံတွင်၌သာ အမြဲတမ်းပြုပြင်ပါ။

သင်၏ Devices များကို သင်္ကေတစာဝှက်လုံခြုံရေးစနစ် (Encrypted) ပြုလုပ်ရန်

- စမတ်ဖုန်းအသစ်များတွင် သင်္ကေတစာဝှက်လုံခြုံရေးစနစ် (Encrypted) ပါရှိသည်။ ၎င်းတို့ကို ချိန်ညှိချက် (Setting) တွင် သေချာစွာဖွင့်ထားပါ။
- Window ရှိ Full-disk Encryption ကို ဖွင့်ထားရန်အတွက် Bitlocker နှင့် Mac အတွက် ဆိုလျှင် Firevault ကို အသုံးပြုပါ။ သို့မဟုတ် Hard Drive နှင့် External Storage များအတွက် အခမဲ့ Veracrypt ကို အသုံးပြုပါ။
- Encrypted ကို အသုံးပြုရန်အတွက် ရှည်လျားထူးခြားသောစကားဝှက် (Long Unique Password)ကို အသုံးပြုပါ။ စမတ်ဖုန်းပေါ်တွင် စိတ်ကြိုက်ချိန်ညှိချက် (Custom Setting) ပြုလုပ်သည့်အခါ ပို၍ ရှည်လျားထူးခြားရှုပ်ထွေးသောစကားဝှက် (Complex Password) ကို အသုံးပြုခြင်းသည် အဓိကသော့ချက်ဖြစ်သည်။
- စကားဝှက်များအကြောင်းကို ကျွမ်းကျင်သောစွမ်းရည်ရှိသည့် သို့မဟုတ် သင့် Device အတွင်းရှိ လျှို့ဝှက်စနစ်ကို အတင်းအကြပ် Decryption လုပ်စေနိုင်သည့် ဆန့်ကျင်ဘက်များက သင်၏ သတင်းအချက်များကို ရယူနိုင်သည်ကို သတိပြုပါ။
- သင် နေထိုင်သောနိုင်ငံ သို့မဟုတ် ခရီးသွားနေသောနိုင်ငံတွင် သင်အသုံးပြုသော Encryption ၏ တရားဝင်မှုရှိမရှိအတွက် သက်ဆိုင်ရာနိုင်ငံ၏ ဥပဒေကို အမြဲတမ်းရှာဖွေလေ့လာပါ။

(၄) သင်္ကေတစာဝှက်လုံခြုံရေးစနစ်ရှိသော ဆက်သွယ်ရေး (Encrypted Communications)

စာနယ်ဇင်းသတင်းသမားများသည် သင်္ကေတစာဝှက်လုံခြုံရေးစနစ် (Encrypted) လုပ်ထားသော စာတိုပေးပို့သည့် အက်ပလီကေးရှင်းများ သို့မဟုတ် အီးမေးလ်များကို Encrypted လုပ်သည့် ဆော့ဖ်ဝဲလ်များကို အသုံးပြုခြင်းတို့ကြောင့် လက်ခံရရှိသူကသာလျှင်ဖတ်နိုင်သဖြင့် အဆက်အသွယ်များကို လုံခြုံစိတ်ချစွာ ဆက်သွယ်နိုင်သည်။ အချို့ Tools များသည် အသုံးပြုရသည်မှာ ပိုမိုလွယ်ကူသည်။ အချို့သော Encrypted ပြုလုပ်ခြင်းအားဖြင့် Message အတွင်းရှိ အချက်အလက်များကို တစ်ပါးသူဖတ်၍ မရနိုင်ရန် ကာကွယ်သည်။ သို့သော် ပါဝင်ပတ်သက်သောသူများ (Companies) အနေဖြင့် Meter Data များဖြစ်သည့် မည်သည့်အချိန်တွင် ပို့သည်၊ မည်သူမှပို့သည်၊ မည်သူကလက်ခံသည် စသည့် အသေးစိတ်အချက်အလက်များကို တွေ့မြင်သိရှိနိုင် သည်။ ၎င်းတို့အနေဖြင့် ဤအချက်အလက်များကို မည်သို့သိမ်းဆည်းထားကြောင်းနှင့် အာဏာပိုင်များက မေးမြန်းသောအခါ မည်သို့တုံ့ပြန်သည်နှင့်ပတ်သက်၍ မူဝါဒအမျိုးမျိုးရှိကြသည်။

မက်ဆေ့ချ် ပို့ခြင်းနှင့် လက်ခံခြင်းတို့အတွက် နှစ်ဘက်စလုံးတွင်သင်္ကေတစာဝှက်လုံခြုံရေးစနစ် (end-to-end Encryption) ထားရှိရန် အကြံပြုသည်။ ဆိုလိုသည်မှာ ပေးပို့သူမှ လက်ခံသူထံ ပေးပို့လိုက်သည့် သတင်းအချက်အလက်များကို Encryption လုပ်၍ ပေးပို့ခြင်းဖြစ်သည်။

နှစ်ဦးနှစ်ဖက်စလုံးတွင် တူညီသော Application ကို အသုံးပြု၍ဖွင့်ထားသည့် အကောင့်တခုစီရှိရပါမည်။ မက်ဆေ့ချ်အား ပေးပို့လက်ခံသော Device အသုံးပြုသူ သို့မဟုတ် အက်ပလီကေးရှင်းနှင့် ချိတ်ဆက်ထားသော အကောင့်၏ စကားဝှက်ကို ရယူသုံးစွဲသူ မည်သူမဆို မက်ဆေ့ချ်ပါအကြောင်းအရာများကို ကြားဖြတ်ရယူနိုင်ဆဲဖြစ်သည်။ ဥပမာအားဖြင့် end-to-end Encryption ဖြင့်အလုပ်လုပ်သော အက်ပလီကေးရှင်းများတွင် Signal, WhatsApp နှင့် Telegram တို့ပါဝင်သည်။

သင်္ကေတစာဝှက်လုံခြုံရေးစနစ် (Encrypted) ကိုအသုံးပြု၍ အီးမေလ်းပေးပို့ခြင်းသည် သတင်းအချက်အလက်များကိုဖလှယ်ရာတွင် ပိုမိုလုံခြုံသောနည်းလမ်းဖြစ်ပါသည်။ နှစ်ဦးနှစ်ဖက်စလုံး Encrypted ကို အသုံးပြု၍ အီးမေးလ်ပို့ခြင်းနှင့် လက်ခံခြင်းအတွက် တူညီသော Software ကို ဒေါင်းလုပ်လုပ်ပြီး Install ရယူထားရမည်ဖြစ်သည်။

သင်္ကေတစာဝှက်လုံခြုံရေးစနစ် (Encrypted) ကို အသုံးပြု၍ စာတိုပေးပို့ရေးအက်ပ်များကို အသုံးပြုရန် -

- အက်ပလီကေးရှင်းကို မည်သူပိုင်ဆိုင်သည်၊ မည်သည့်အသုံးပြုသူ၏ အချက်အလက်များကိုသိမ်းဆည်း ထားသည်နှင့် ထိုအချက်အလက်များကို အစိုးရက တောင်းဆိုရယူခြင်းရှိမရှိတို့ကို ဆန်းစစ်လေ့လာ ထားသင့်ပါသည်။ ထို့အပြင် အသုံးပြုသူများ၏ အချက်အလက်များကိုမျှဝေရန် တောင်းဆိုမှုများကို တုန့်ပြန်ရန်အတွက် မည်သို့သောမူဝါဒများရှိကြောင်းကိုသိရန်လည်း ဆန်းစစ်လေ့လာပါ။
- သင့်ဖုန်းကိုခိုးယူခြင်းခံရလျှင် တစ်စုံတစ်ယောက်ကဖွင့်ယူအသုံးပြုခြင်းမှကာကွယ်ရန် ဖြစ်နိုင်ပါက အက်ပလီကေးရှင်းဖြင့် PIN သို့မဟုတ် Password ကိုသုံးပါ။
- သင်၏ မက်ဆေ့ချ် အက်ပလီကေးရှင်းများမှပေးပို့သည့် အချက်အလက်များကို သင့်ဖုန်းထဲရှိ မည်သည့်နေရာတွင် သိမ်းဆည်းထားသည်ကို သိရှိပါ။
- သင်သည် ဓာတ်ပုံများကဲ့သို့ ဒေါင်းလုတ်လုပ်သမျှသည် သင်၏ Device ပေါ်တွင်သိမ်းဆည်းထားပြီး၊ အခြား Device များနှင့် အက်ပ်များသို့လည်းကူးယူနိုင်သည်။ အထူးသဖြင့် သင့်ဒေတာကို Back up လုပ်သည့်အခါမျိုးဌ ထိုကဲ့သို့ကူးယူထားနိုင်သည်။
- WhatsApp ကဲ့သို့ ဝန်ဆောင်မှုအချို့သည် တယ်လီဖုန်းနံပါတ်နှင့်ချိတ်ဆက်ထားသော Cloud Account ထဲ၌ သင်၏ မက်ဆေ့ချ်ကိုအရန်သိမ်းဆည်းပေးသည်။
- သင်၏ဖုန်းထဲတွင်သိမ်းဆည်းထားသည့်အဆက်အသွယ်များသည် Messaging App နှင့် Cloud Account များနှင့် တစ်ပြိုင်တည်းချိတ်ဆက်ခြင်းပြုလုပ်နိုင်သောကြောင့် တစ်နေရာ၌ သင်ဖျက်ရန်ကြိုးစားသည့် နံပါတ်များကို အခြားနေရာများတွင်သိမ်းထားနိုင်သည်။
- မက်ဆေ့ချ်များသိမ်းဆည်းခြင်းနှင့် ဖျက်သိမ်းခြင်းတို့ကို ပုံမှန်ပြုလုပ်ခြင်းဖြင့် Device တစ်ခု သို့မဟုတ် အကောင့်တစ်ခုတွင် တတ်နိုင်သမျှအနည်းဆုံးသိမ်းဆည်းထားသိထားပါ။။ မှတ်တမ်းများနှင့် မာလ်တီမီဒီယာမက်ဆေ့ချ်များအပါအဝင် သိမ်းဆည်းထားသည့်အရာများကို

ပြန်လည်သုံးသပ်ရန် လုပ်ငန်းစဉ်တစ်ခုကိုဖန်တီးပါ။ Downloads များ သို့မဟုတ် Screenshots များကို Encrypted လုပ်ထားသော External Storage Device တွင် သိမ်းဆည်းပါ။

- Signal ၏ ပျောက်ကွယ်အောင်ပြုလုပ်ပေးသော လုပ်ဆောင်ချက်များက သင်၏ မက်ဆေ့ချ်များကို အချိန်ကာလတစ်ခု၌ အလိုအလျောက်ပျောက်ကွယ်သွားအောင် ပြုလုပ်ပေးသည်။

သင်္ကေတစာဝှက်လုံခြုံရေးစနစ်ရှိသော အီးမေးလ် (Encrypted email)ကို သုံးစွဲရန် -

- နည်းပညာကျွမ်းကျင်သည့် ယုံကြည်စိတ်ချရသော အဆက်အသွယ်ထံမှ အကူအညီကိုရယူပါ။ သင့်အတွက် အသစ်အဆန်းဖြစ်နေသည်ဆိုလျှင် သင်္ကေတစာဝှက်လုံခြုံရေးစနစ်ရှိသော အီးမေးလ် (Encrypted email) စနစ်သည် Set up ပြုလုပ်ရန် အမြဲတမ်းမလွယ်ကူပါ။
- နည်းပညာနားလည်သူများသုံးသပ်ထားပြီး နာမည်ရသော သင်္ကေတစာဝှက်လုံခြုံရေးစနစ်ရှိသော အီးမေးလ် (Encrypted email) သုံး ဆော့ဖ်ဝဲလ်များကိုရွေးချယ်ပါ။
  လုံခြုံရေးအားနည်းချက်များကို ကာကွယ်ရန် သင်၏ ဆော့ဖ်ဝဲလ်များကို အမြဲတမ်း အဆင့်မြှင့်တင် (Update) လုပ်ပါ။
- သင်္ကေတစာဝှက်လုံခြုံရေးစနစ်သုံး ဆော့ဖ်ဝဲလ် (Encrypted Email Software) ကိုအသုံးပြုရန် ရှည်လျားထူးခြားသောစကားဝှက် (Long Unique Password)ကို ကြိုတင်အချိန်ယူဖန်တီးပါ။ ထိုစကားဝှက်ကို မေ့သွားပါက Encrypted email သို့ ဝင်ရောက်နိုင်ခွင့်ကို ဆုံးရှုံးသွားလိမ့်မည်။
- အီးမေးလ်များပို့လျှင် ပုံမှန် Encrypted လုပ်ပြီး ပို့ခြင်းအားဖြင့် ဆော့ဖ်ဝဲလ်များကို မည်သို့အသုံးပြုရမည်ကို မမေ့တော့ပါ။
- အီးမေးလ်၏ ခေါင်းစဉ်၊ မက်ဆေ့ချ် ပေးပို့သူနှင့် လက်ခံသူတို့၏ အီးမေးလ်လိပ်စာများအပါအဝင် အသေးစိတ်အချက်အလက်များကို Encrypted မလုပ်ထားပါ။

ဥပမာအားဖြင့် သင်္ကေတစာဝှက်လုံခြုံရေးစနစ်သုံး ဆော့ဖ်ဝဲလ် (Encrypted Email Software) တွင် Mac အတွက် GPG Suite ကိုသုံးရန်၊ Windows နှင့် Linux , Enigmail extension ပါသော Thunderbird နှင့် Mailvelope တို့အတွက် GPG4win ကိုသုံးရန် ဖြစ်သည်။

(၅) လုံခြုံသော အင်တာနက်သုံးစွဲမှု (Secure Internet Use)

စာနယ်ဇင်းသတင်းသမားများသည် အင်တာနက်ကိုမှီခိုသော်လည်း အင်တာနက်ဝန်ဆောင်မှုပေးသူ များ၊ အင်တာနက်ကဖေးများ၊ ဟိုတယ်များရှိအခမဲ့ WiFi များအား သူတို့၏ အွန်လိုင်းအသုံးပြုလုပ်ဆောင်မှုများ ကို မျှဝေလိုမည်မဟုတ်ပါ။ ဒုစရိုက်သမားများသာမက အဆင့်မြင့်နည်းပညာသုံး ဆန့်ကျင်ဘက် (Sophisticated Adversaries) များသည် မလုံခြုံသော

ဝက်ဘ်ဆိုက်များ သို့မဟုတ် အများပြည်သူသုံး WiFi ဆက်သွယ်မှုများကိုအသုံးပြု၍ သတင်းအချက်အလက်များကို ခိုးယူခြင်း၊ စောင့်ကြည့်ခြင်းတို့ ပြုလုပ်နိုင်သည်။

အင်တာနက်ကို လုံခြုံစွာအသုံးပြုရန်

- ဝက်ဘ်ဆိုက်လိပ်စာ URL (https://cpj.org) ၏ အစတွင် https နှင့် သော့ခလောက်ပုံသင်္ကေတ (Padlock Icon) ကို ရှာဖွေပါ။ ၎င်းသည် သင်နှင့် သွားရောက်နေသောဝက်ဘ်ဆိုက်ကြား ရှိအသွားအလာကို သင်္ကေတစာဝှက်လုံခြုံရေး (Encrypted) လုပ်ထားကြောင်း ညွှန်ပြသည်။ သင်ကြည့်ရှုသော ဝက်ဘ်ဆိုက်များသည် လုံခြုံမှုရှိမရှိကို Electronic Frontier Foundation ၏ HTTPS Everywhere Browser Extension ကိုအသုံးပြုပြီး အမြဲတမ်းစစ်ဆေးပါ။
- ဝက်ဘ်ဆိုက်လိပ်စာသည် အစစ်အမှန်ဖြစ်ကြောင်း၊ အတုအယောင်မဟုတ်ကြောင်းကိုလည်း စစ်ဆေးပါ။ URL ကို မှန်ကန်စွာစာလုံးပေါင်းပြီး https ပါဝင်ရမည်။
- Pop-up ကြော်ငြာများ၏ နောက်ကွယ်၌ လျှို့ဝှက်စွာကပ်ပါလာလေ့ရှိသည့် အန္တရာယ်ပေးသောဆော့ဖ် ဝဲလ် (Malware) ကို ကာကွယ်နိုင်ရန်အတွက် Ad-Blocker ကို ထည့်သွင်းထားပါ။ Ad-Blockers များသည် အချို့ဆိုဒ်များအားပိတ်ဆို့ခြင်းမှ ကင်းလွတ်ခွင့်ပြုထားသည်။
- အွန်လိုင်းပေါ်တွင် မည်သည့်ဝက်ဘ်ဆိုက်ထဲသို့ ဝင်ရောက်ခဲ့သည်ကိုခြေရာခံနိုင်သည့် ဝက်ဘ်ဆိုက်နှင့် ကြော်ငြာများကိုတားဆီးရန်အတွက် Privacy Badger ကို ထည့်သွင်းထားပါ။
- အသုံးမပြုသည့်အခါ Bluetooth နှင့်အခြား ဖိုင်မျှဝေသည့်အက်ပ်များ (File-sharing Apps)နှင့် ဝန်ဆောင်မှုများကိုပိတ်ပါ။
- အင်တာနက်လမ်းကြောင်းကို ကာကွယ်ရန် VPN ကိုသုံးပါ။ အထူးသဖြင့် လုံခြုံမှုမရှိသော အများသုံး WiFi ကိုသုံးစွဲနေစဉ်တွင် သင့်အား ဟက် (Hack)လုပ်ခြင်း သို့မဟုတ် စောင့်ကြည့်ခြင်းကိုခံရနိုင်သည်။
- အများသုံး ကွန်ပျူတာများ၊ အထူးသဖြင့် အင်တာနက်ကဖေးများ သို့မဟုတ် သတင်းထုတ်ပြန်ရေးဌာန များရှိ ကွန်ပျူတာများကို အသုံးပြုခြင်းမှရှောင်ကြဉ်ပါ။ အကယ်၍ မရှိမဖြစ်အသုံးပြုရမည်ဆိုပါက မိမိအသုံးပြုခဲ့သမျှမှ ထွက်ခဲ့ပြီး (Log out) သင်၏ ဝင်ရောက်အသုံးပြုခြင်းရာဇဝင်ကို ရှင်းလင်းခဲ့ပါ။
- အင်တာနက်အသုံးပြုခြင်းကို အမည်မဖော်လိုသူ သို့မဟုတ် Tails အဖြစ်သုံးနိုင်ရန် Tor Browser Bundle ကို install လုပ်ရန်စဉ်းစားပါ။ ၎င်းသည် သင်၏ အင်တာနက်အသွားအလာအားလုံးကို Tor မှတစ်ဆင့်ဖြတ်သန်းသွားစေသည့် အခမဲ့လည်ပတ်ဆောင်ရွက်မှုစနစ် (A free operating system) ဖြစ်သည်။ နိုင်ငံများရှိ အဆင့်မြင့်အစိုးရပိုင်း အကျင့်ပျက်ခြစားမှုများကဲ့သို့ အကဲဆတ်သော အကြောင်းအရာများကို စုံစမ်းစစ်ဆေးသတင်းရယူသည့် စာနယ်ဇင်းသတင်းသမားများအတွက် Tor ကိုအသုံးပြုရန် အထူးအကြံပြုသည်။

(၆) ပြည်ပဝင်ထွက်ပေါက်(နယ်စပ်)များကို ဖြတ်ကျော်ခြင်း (Crossing Borders)

စာနယ်ဇင်းသတင်းသမားများသည် အလုပ်နှင့်ကိုယ်ရေးကိုယ်တာ အချက်အလက်များကို သယ်ဆောင်ပြီး နယ်စပ်ကိုဖြစ်ကျော်စဉ် ၎င်းတို့၏ အီလက်ထရောနစ်ကိရိယာများ (Electronic Devices) ကို အခြားသူများက ရရှိသွားမည်ကိုမလိုလားပေ။ အကယ်၍ နယ်ခြားစောင့်အဖွဲ့များက စက်ပစ္စည်းတစ်ခုခုကို သင့်မျက်မှောက်မှ ယူဆောင်သွားလျှင် ၎င်းတို့အနေဖြင့် ထိုပစ္စည်းများကို ရှာဖွေရန်၊ အကောင့်များအတွင်းသို့ ဝင်ရောက်နိုင်ရန်နှင့် သတင်းအချက်အလက်များကို မူပွားကူးယူရန် သို့မဟုတ် ထောက်လှမ်းသည့်ဆော့ဖ်ဝဲလ် (Spyware) များကို ထည့်သွင်းပေးနိုင်ရန် အခွင့်သာသွားလိမ့်မည်။ **အမေရိကန်နယ်စပ်ကို ဖြတ်သန်းသော စာနယ်ဇင်းသတင်းသမားများအနေနှင့် CPJ ၏ လုံခြုံရေးမှတ်စု 'Nothing to Declare' တွင် အကြံဉာဏ်ယူပါ။**

သင် ခရီးမထွက်ခွာမီ -

- သင်၏ Devices များထဲတွင် မည်သည့်သတင်းအချက်အလက်များကို ထည့်သွင်းထားသည်၊ ၎င်းအချက်အလက်များသည် သင်နှင့် သင့်အဆက်အသွယ်များကို မည်သို့အန္တရာယ်ပေးနိုင်သည်ကို သိရှိထားပါ။ ၎င်း Devices များသည် သင်၏ ခရီးသွားအိတ်ထဲတွင်ပါရှိသော မှတ်စုများနှင့် အခြား ပုံနှိပ်စာရွက်စာတမ်းများကဲ့သို့ တူညီသောစစ်ဆေးမှုကိုခံရနိုင်သည်ဟု မှတ်ယူထားပါ။
- သင်၏ Devices များအားလုံးကို External hard drive သို့မဟုတ် Cloud ထဲသို့အရန်ကူးယူထားပါ။
  နယ်စပ်စစ်ဆေးရေးအရာရှိများက ဝင်ရောက်မကြည့်ရှုစေလိုသော အချက်အလက်များကို သင်၏ Devices များထဲမှာ ဖယ်ရှားထားပါ။
- ဖြစ်နိုင်လျှင် ခရီးသွားရာတွင်အသုံးပြုရန်အတွက် သီးသန့် Devices များကို ဝယ်ယူအသုံးပြုပါ။ အထူးသဖြင့် အလွန်အကဲဆတ်သော အကြောင်းအရာကိစ္စများကိုသတင်းရယူရန် ဆောင်ရွက်နေစဉ် တွင်ဖြစ်သည်။ အကယ်၍ ကိုယ်ရေးကိုယ်တာ သို့မဟုတ် အလုပ်နဲ့ပတ်သက်သော Devices များကို ယူဆောင်ပြီး ခရီးသွားပါက ၎င်းထဲရှိအချက်အလက်များကို လုံခြုံစွာ အရန်သိမ်းဆည်းခြင်း (Back up) လုပ်ထားပြီးနောက် ၎င်းတို့ကို ဖယ်ရှားရှင်းလင်းပါ။ သို့မဟုတ် အစမှပြန်လည်စတင်မှု (Reset) လုပ်ပါ။
- စကားဝှက်မပါပဲ သင်၏သတင်းအချက်အလက်များကို ဝင်ရောက်နိုင်ခြင်းမရှိစေဖို့ သေချာစေရန် Devices များအားလုံးအတွက် အပြည့်စာဝှက်လုံခြုံရေးစနစ် (full-disk Encryption) ကိုဖွင့်ထားပါ။ မည်သည့်ဥပဒေကိုမျှ ချိုးဖောက်မှုမရှိကြောင်း သေချာစေရန် သင်ရောက်ရှိနေသော တိုင်းပြည်၏ Encryption နှင့် ပတ်သက်သော ကန့်သတ်ချက်များကို လေ့လာထားပါ။

လုံခြုံရေးတပ်ဖွဲ့များသည် သင်၏ စကားဝှက်အား တရားဝင်တောင်းခံနိုင်သည်ကို သတိပြုပါ။ အကယ်၍ သင်သည် ပြည်ပဝင်ထွက်ပေါက်(နယ်စပ်)ကိုဖြတ်ကျော်စဉ် တားမြစ်ခံရနိုင်ဖွယ်ရှိပါက ခရီးမသွားမီ သင်၏ အလုပ်ရှင် သို့မဟုတ် ရှေ့နေထံမှ အကြံဉာဏ်များကို ရယူထားပါ။

- Devices များအတွင်းရှိ သင်၏ အကောင့်များအားလုံးကို ထွက်ထား (Log out)ပါ။ နယ်စပ်ကို ဖြတ်ပြီးသည့်တိုင်အောင်နှင့် လုံခြုံသောအင်တာနက်အဆက်အသွယ်မူသို့မရောက်မချင်းတိုင်အောင် Application များကို ဖယ်ထုတ်ထားပါ။
- သင်၏ Devices များပေါ်ရှိ **အသုံးပြုဝင်ရောက်မှုရာဇဝင် (Browsing History)** ကို **ရှင်းလင်းထားပါ။ (အင်တာနက်ဝန်ဆောင်မှုပေးသူသည် သင်ကြည့်ရှုခဲ့သော ဝဘ်ဆိုဒ်များကို** မှတ်တမ်းတင်ထားဆဲ ဖြစ်သည်။)
- ကိရိယာအားလုံးကို သော့ခတ် (Lock) ထားရာတွင် သင်၏ မျက်နှာ သို့မဟုတ် လက်ဗွေများကဲ့သို့သော ဇီဝဗေဒဆိုင်ရာအချက်အလက်များအစား PIN နံပါတ် သို့မဟုတ် လျှို့ဝှက်နံပါတ်ဖြင့် အသုံးပြုပါ။
- အကယ်၍ သင် ဖမ်းဆီးထိန်းသိမ်းခံရပါက သင်၏ Devices အတွင်းရှိ အချက်အလက်များကို အဝေးနေရာမှ ရှင်းလင်းဖယ်ရှားပစ်ရန် ယုံကြည်စိတ်ချရသူတစ်ဦးကို ရှင်းလင်းသောညွှန်ကြားချက်များကို ပေးထားပါ။

ပြည်ပဝင်ထွက်ပေါက်(နယ်စပ်)တွင် -

- Disk Encryption ကိုအသက်ဝင်စေရန် သင်၏ Devices များကိုပိတ်ထားပါ။
- လုံခြုံရေးကိုဖြတ်သန်းနေစဉ် သင်၏ Devices များကို မျက်ခြေမပြတ်ပါစေနှင့်။
- လေဆိပ်မှ အဝေးသို့မရောက်မချင်း သင့်ဖုန်းကို မဖွင့်ပါနှင့်။ မည်သည့် ဖုန်းခေါ်ဆိုခြင်းနှင့် SMS မက်ဆေ့ချ်များကိုမဆို ဒေသတွင်းဝန်ဆောင်မှုပေးသူမှတစ်ဆင့် ဖြတ်သန်းသွားမည်ဖြစ်သည်။ ၎င်းဝန်ဆောင်သူများသည် အချက်အလက်များကိုရယူပြီး အာဏာပိုင်များကို မျှဝေနိုင်သည်။ လေဆိပ် WiFi နှင့်ဆက်သွယ်အသုံးပြုစဉ်တွင် VPN ကို အသုံးပြုပါ။
- ပြည်ပဝင်ထွက်ပေါက်(နယ်စပ်)တွင် မည်သည့် Devices များကိုမဆို သိမ်းဆည်းခံရပါက သို့မဟုတ် ၎င်းထဲသို့ တစ်ခုခုထည့်သွင်းခံရပါက ၎င်းတွင် အားနည်းချက်ရှိသွားသည်ဟုယူဆနိုင်ပြီး ၎င်းအတွင်းရှိ မည်သည့်အချက်အလက်ကို မဆိုကူးယူခြင်း ခံထားရသည်ဟုမှတ်ယူပါ။

အယ်ဒီတာမှတ်စု

ဤအချက်များကို မူလက ၂၀၁၁ ခုနှစ်၊ ဇူလိုင်လ ၃၀ ရက်တွင် ပုံနှိပ်ထုတ်ဝေခဲ့ပြီး၊ တိကျမှန်ကန်မှုရှိမရှိကို အပေါ်ဆုံးတွင်ဖော်ပြထားသည့်နေ့စွဲတွင် ပြန်လည်သုံးသပ်သည်။