EFF'S SURVEILLANCE SELF-DEFENSE

သူခိုးဆော့ဖ်ဝဲများ၏ ရုန်မှ ဘယ်လို ကာကွယ်မလဲ။

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

LOCALIZATION LAB

သူခိုးဆော့ဖ်ဝဲများ၏ ရန်မှ ဘယ်လိုကာကွယ်မလဲ။

နောက်ဆုံးစိစစ်ထားသည့် ရက်စွဲ - ၂၀၂၁ ခုနှစ် ဇွန်လ ၂၅ ရက်

သူခိုးဆော့ဖ်ဝဲ (malicious software ကို အတိုကောက် malware ဟုသုံးနှုန်းသည်။) ဆိုသည်မှာ ကွန်ပျူတာ သုံးစွဲသူများကို ထိခိုက်နစ်နာစေရန် အသုံးပြုတဲ့ ဆော့ဖ်ဝဲဖြစ်ပါတယ်။ အောက်ပါတို့အပါအဝင် သူခိုးဆော့ဖ်ဝဲ များ လုပ်ဆောင်နိုင်တဲ့ ကိစ္စအများအပြားရှိပါတယ်။

- ကွန်ပျူတာလည်ပတ်မှုကို နှောင့်ယှက်ခြင်း
- အရေးကြီးတဲ့ သတင်းအချက်အလက်များကို နှိုက်ယူခြင်း
- သုံးစွဲသူဟန်ဆောင်ပြီး spam သို့မဟုတ် စာအတုများ ပို့ခြင်း
- ပုဂ္ဂလိက ကွန်ပျူတာစနစ်များကို ခိုး၍ဝင်ရောက်ခြင်း

သူခိုးဆော့ဖ်ဝဲအများစုသည် တရားဝင်ခြင်းမရှိပါ။ ဘဏ်နှင့်ပတ်သက်သော အချက်အလက်များ၊ အီးမေးလ် သို့မဟုတ် လူမှုကွန်ယက်များသို့ ဝင်ရောက်ရာတွင် ဖြည့်စွက်ရသည့် အချက်အလက်များ စသည်တို့ကို ခိုးယူရန် အသုံးပြုကြပါတယ်။ အစိုးရများ၊ တရားဥပဒေစိုးမိုးရေး အေဂျင်စီများသာမက သာမန်လူများ ကပါ ကုဒ်ဖြင့်ပြောင်းလဲမှု ကို ဖြတ်ကျော်ပြီး အခြားသူများကို လျှို့ဝှက်ထောက်လှမ်းရန် သူခိုးဆော့ဖ်ဝဲကို အသုံးပြု ကြပါတယ်။ အနှောင့်အယှက် ပေးလိုသူက သူခိုးဆော့ဖ်ဝဲအသုံးပြုပြီး ဝက်ဘ်ကင်မရာနဲ့ မိုက်ခရိုဖုန်း တို့ကနေ တစ်ဆင့် ရုပ်သံမှတ်တမ်း ကူးယူခြင်း၊ ဗိုင်းရပ်စ်တန်ပြန်ခြင်း ပရိုဂရမ်များရဲ့ အန္တရာယ်ရှိကြောင်း အသိပေးမှု စနစ်ကို ဖြုတ်ပစ်ခြင်း၊ ကွန်ပျူတာခလုပ်ခုံမှာ ရိုက်ထည့်လိုက်သော အကြောင်းအရာများကို ကူးယူခြင်း၊ အီးမေးလ် နဲ့ အခြား စာရွက်စာတမ်းများကို ကူးယူခြင်း၊ စကားဝှက်များ ခိုးယူခြင်း စတဲ့ ကိစ္စများစွာကို လုပ်ဆောင် နိုင်ပါတယ်။

အနှောင့်အယှက်သည် သူခိုးဆော့ဖ်ဝဲကိုသုံး၍ မိမိအား ဘယ်လိုပစ်မှတ်ထား တိုက်ခိုက်လာနိုင်သနည်း။

သူခိုးဆော့ဖ်ဝဲရဲ့ တိုက်ခိုက်မှု ကို ကာကွယ်ဖို့ အကောင်းဆုံးနည်းလမ်းဟာ အစကတည်းက မိမိရဲ့စက်ပစ္စည်းများ ပေါ်ကို ကူးမလာအောင် ဂရုစိုက်ခြင်းဖြစ်တယ်။ ဒါပေမယ့်

ကိုယ့်ကိုအနှောင့်ယှက်ပေးသူက ဖန်တီးသူမသိရှိ လိုက်သောချို့ယွင်းချက် ကဲ့သို့ ဟာကွက်များကို ဝင်ရောက်နိုင်လျှင် ကာကွယ်ဖို့ခက်ခဲနိုင်ပါတယ်။ ကွန်ပျူတာ ဆော့ဖ်ဝဲတစ်ခုမှာ ယခင်ဘယ်သူမှ မသိထားတဲ့ ဟာကွက်တွေကို အသုံးချပြီး တိုက်ခိုက်မှုတွေ ပြုလုပ်လာနိုင် ပါတယ်။ မိမိရဲ့ကွန်ပျူတာကို ခံတပ်တစ်ခုလို့မြင်ကြည့်ပါ။ ဖန်တီးသူမသိရှိလိုက်သော ချို့ယွင်းချက် ဆိုသည်မှာ မိမိက မသိရှိပေမဲ့လည်း တိုက်ခိုက်သူက ရှာဖွေတွေ့ရှိထားတဲ့ လျှို့ဝှက်တံခါးပေါက်လိုမျိုး ဖြစ်ပါတယ်။ ကိုယ်ကိုတိုင် ရှိမှန်းမသိတဲ့ အပေါက်ကနေ ဝင်ရောက်လာတဲ့အတွက် ကြိုတင်ကာကွယ်လို့ မရနိုင်ပါဘူး။ သူခိုးဆော့ဖ်ဝဲ အသုံးပြုပြီး ပစ်မှတ်ထားတိုက်ခိုက်မှုများ ပြုလုပ်ဖို့ အစိုးရနှင့် တရားဥပဒေစိုးမိုးရေး အေဂျင်စီကဲ့သို့သော အဖွဲ့တွေက ဒီလိုမျိုး ဖန်တီးသူမသိရှိလိုက်သော ချို့ယွင်းချက်များကို ရှာဖွေစုစည်းထားလေ့ရှိပါတယ်။ ရာဇဝတ်သမားတွေ နဲ့ အခြားမသမာသူတွေကလည်း မိမိကွန်ပျူတာပေါ်မှာ သူခိုးဆော့ဖ်ဝဲကို ခိုးပြီးတပ်ဆင်ဖို့အတွက် ဖန်တီးသူမသိရှိ လိုက်သော ချို့ယွင်းချက်များကို သုံးလေ့ရှိကြပါတယ်။ ဒါပေမယ့် ဖန်တီးသူမသိရှိလိုက်သော ချို့ယွင်းချက်များကို ဝယ်ယူဖို့ ဈေးကြီးပြီး ထပ်တလဲလဲသုံးဖို့လည်း ခက်ခဲတယ် (လျှို့ဝှက်တံခါးပေါက်ကနေ တစ်ခါခိုးဝင်ပြီးရင် ဒီအပေါက်ကို တစ်ခြားသူတွေကလည်း ရှာတွေ့နိုင်ခြေ မြင့်လာပါတယ်)။ ဒါ့ကြောင့် ဒီနည်းသုံးမယ့်အစား ကိုယ့်ဘာသာကိုယ် မသိလိုက်ဘဲ သူခိုးဆော့ဖ်ဝဲကို တပ်မိသွားအောင် လှည့်ဖျားတဲ့နည်းလမ်း ပိုအသုံးပြုကြ ပါတယ်။

ကိုယ်မသိလိုက်ဘဲ ကွန်ပျူတာပေါ်မှာ သူခိုးဆော့ဖ်ဝဲ တပ်မိသွားအောင် လှည့်ဖျားတဲ့ နည်းလမ်းမျိုးစုံ ရှိပါတယ်။ သူခိုးဆော့ဖ်ဝဲကို ဝက်ဘ်ဆိုဒ်တစ်ခုရဲ့ လင့်ခ်၊ စာရွက်စာတမ်း၊ PDF ၊ ကွန်ပျူ တာလုံခြုံရေးပရိုဂရမ်တစ်ခု စသည်ဖြင့် အမျိုးဆုံး အယောင်ဆောင်ပြီး ပေးပို့လာနိုင်ပါတယ်။ အီးမေးလ် (ကိုယ်နဲ့ သိသူ တစ်ယောက်က ပေးပို့ဟန်ဆောင်ပြီး)၊ Skype ၊ Twitter စတဲ့ ချက်ချင်းပို့စာစနစ်များ၊ ကိုယ့်ရဲ့ Facebook စာမျက်နှာပေါ် လာတင်သည့် လင့်ခ် စသည့်လမ်းကြောင်းများမှတစ်ဆင့် ပေးပို့လာနိုင်ပါတယ်။ ကိုယ့်ကို ပစ်မှတ်ထားမှု ကြီးလေလေ သူခိုးဆော့ဖ်ဝဲကို အစစ်နှင့်အတုမခွဲခြားမိဘဲ ကူးဆွဲမိအောင် ကြိုးစားလာလေလေ ဖြစ်ပါလိမ့်မယ်။

ဥပမာပေးရရင် လက်ဘနွန်နိုင်ငံမှာ ဟတ်ကာများဟာ ပြည်သူတွေကို ပစ်မှတ်ထားဖို့အတွက် Signal ၊ WhatsApp အစရှိတဲ့ လုံခြုံတဲ့ ဆက်သွယ်ရေးနည်းပညာတွေကို အတု ပြုလုပ်ပြီး သူခိုးဆော့ဖ်ဝဲကို ခိုးထည့်ဖြန့်ချိ ကြပါတယ်။ အီဘီယိုးပီးယားနိုင်ငံမှာဆိုရင် နိုင်ငံရေးလှုပ်ရှားသူများ၊ ကျောင်းသူကျောင်းသားများ၊ လူ့အခွင့်အရေးဆိုင်ရာ ဥပဒေပညာရှင်များဟာ Adobe Flash update တွေ၊ နိုင်ငံရေးသတင်း အချက် အလက် များ ပါတဲ့ PDF ဖိုင်တွေ ဟန်ဆောင်ထားတဲ့ ထောက်လှမ်းရေးဆော့ဖ်ဝဲတွေ နဲ့ ပစ်မှတ်ထား တိုက်ခိုက်ခံခဲ့ရပါတယ်။ တိဗက်အရေး လှုပ်ရှားသူများဟာလည်း အခြားလှုပ်ရှားသူတစ်ယောက်က ပေးပို့တဲ့ PDF ဖိုင်ဟန်ဆောင်ထားတဲ့ သူခိုးဆော့ဖ်ဝဲတွေနဲ့ ပစ်မှတ်ထား တိုက်ခိုက်ခြင်း ခံခဲ့ရပါတယ်။

ဒါဆိုသူခိုးဆော့ဖ်ဝဲရန်ကနေ ကိုယ့်ကိုယ်ကို ဘယ်လိုကာကွယ်မလဲ။

ဗိုင်းရပ်စ်တန်ပြန်ခြင်း ဆော့ဖ်ဝဲသုံးပါ။

ဗိုင်းရပ်စ်တန်ပြန်ခြင်း ဆော့ဖ်ဝဲဟာ “ပစ်မှတ်ထားတိုက်ခိုက်ခြင်း မဟုတ်ဘဲ” လူရာပေါင်း ထောင်ပေါင်းများစွာစီ ဖြန့်ချိဖို့သုံးတဲ့ သာမန် သူခိုးဆော့ဖ်ဝဲတွေကို ခုခံကာကွယ်တဲ့အခါမှာ ထိရောက်ပါတယ်။ ဒါပေမယ့် တရုတ်အစိုးရ ရဲ့ဟတ်ကာများက New York Times သတင်းစာတိုက်ကို တိုက်ခိုက်ဖို့ သုံးတဲ့ ဆော့ဖ်ဝဲလိုမျိုး ပစ်မှတ်ထား တိုက်ခိုက်မှုတွေကို တန်ပြန်ဖို့အတွက်တော့ ထိရောက်မှုမရှိတတ်ပါဘူး။ EFF အနေနဲ့ကတော့ ဘယ်ဆော့ဖ်ဝဲက ပိုကောင်းသလဲ အကြံမပေးနိုင်ပေမယ့် ကွန်ပျူတာနဲ့ ဖုန်းပေါ်မှာ ဗိုင်းရပ်စ်တန်ပြန်ခြင်း ဆော့ဖ်ဝဲတစ်ခုခု အသုံးပြုဖို့ အကြံပြုပါတယ်။

သံသယဖြစ်စရာ ဖိုင်တွဲများကို ဂရုပြုပါ။

ပစ်မှတ်ထား တိုက်ခိုက်သော သူခိုးဆော့ဖ်ဝဲများရန်ကနေ ကာကွယ်ဖို့ အကောင်းဆုံးနည်းလမ်းမှာ သံသယဖြစ် ဖွယ် ဖိုင်တွဲများကို ဖွင့်ကြည့်ခြင်း မပြုလုပ်ရန်ဖြစ်ပါတယ်။ ဖိုင်တွဲတွေကနေတစ်ဆင့် သူခိုးဆော့ဖ်ဝဲများ ပေးပို့ တတ်တဲ့ အတွက်ကြောင့်ဖြစ်ပါတယ်။ ကွန်ပျူတာနဲ့ နည်းပညာကျွမ်းကျင်မှုရှိသူတွေကတော့ ဘယ်ဟာက သူခိုးဆော့ဖ်ဝဲဖြစ်နိုင်တယ် ဆိုတာကို အကဲခတ်နိုင်လောက်ပေမယ့် တစ်ချို့ပစ်မှတ်ထား တိုက်ခိုက်မှုတွေဟာ အစစ်နဲ့အတု တော်တော်ခွဲခြားရခက်ပါတယ်။

ကိုယ်က Gmail အသုံးပြုတယ်ဆိုရင် သံသယဖြစ်ဖွယ် ဖိုင်တွဲတွေကို ကွန်ပျူတာပေါ် ကူးဆွဲခြင်းမပြုဘဲ Google Drive ပေါ်မှာ ဖွင့်ကြည့်သင့်ပါတယ်။ ဒါဆိုကွန်ပျူတာပေါ် သူခိုးဆော့ဖ်ဝဲ ကူးဆက်ခြင်းကို ကာကွယ်ဖို့ အထောက် အကူဖြစ်နိုင်ပါတယ်။ လူသုံးသိပ်မများတဲ့ Ubuntu သို့မဟုတ် ChromeOS လို computing ပလက်ဖောင်းသုံးရင် သာမန်သူခိုးဆော့ဖ်ဝဲတိုက်ခိုက်မှု အန္တရာယ်မှ သိသိသာသာ ကာကွယ်ပေးနိုင်ပေမယ့် အလွန်အဆင့်မြင့်တဲ့ တိုက်ခိုက်မှုတွေရန်ကတော့ ကာကွယ်ပေးနိုင်မှာ မဟုတ်ပါဘူး။

ဆော့ဖ်ဝဲများကို update လုပ်ပါ။

သူခိုးဆော့ဖ်ဝဲရန်က ကာကွယ်ဖို့ နောက်ထပ်လုပ်နိုင်တာတစ်ခုက ကွန်ပျူတာမှာသုံးတဲ့ ဆော့ဖ်ဝဲတွေဟာ နောက်ဆုံးထွက်ရှိထားတာ ဖြစ်စေဖို့နဲ့ နောက်ဆုံးပြင်ဆင်ထားတဲ့ လုံခြုံရေးဆိုင်ရာ အစီအမံများကို ကူးဆွဲ အသုံးပြုဖို့ဖြစ်ပါတယ်။

ဆော့ဖ်ဝဲတွေမှာ ချို့ယွင်းချက်တွေ တွေ့ရှိလာတာနဲ့အမျှ ဆော့ဖ်ဝဲရေးဆွဲသူကုမ္ပဏီတွေဟာ ယင်းပြဿနာများကို ဖြေရှင်းဖို့ ဆော့ဖ်ဝဲ update တွေ လုပ်ခိုင်းလေ့ရှိပါတယ်။ ဒါပေမယ့် ဆော့ဖ်ဝဲ update တွေကို ကိုယ်က ကွန်ပျူတာပေါ်မှာ ကူးဆွဲတပ်ဆင်မှု မလုပ်ရင်တော့ ချို့ယွင်းချက်တွေကို ပြင်ဆင်နိုင်မှာ မဟုတ်ပါဘူး။ လူအများထင်ကြ တာက မှတ်ပုံမတင်ထားတဲ့ ဝင်းဒိုးဆော့ဖ်ဝဲ သုံးစွဲနေရင် လုံခြုံရေးဆိုင်ရာ update တွေ လုပ်လို့မရဘူးလို့ ထင်တတ်ကြပါတယ်။ ဒါဟာမဟုတ်ပါဘူး။

လုံခြုံရေးကျိုးပေါက်မှုဆိုင်ရာ လက္ခဏာများ ကို သတိပြုပါ။

တစ်ခါတစ်ရံမှာ ဗိုင်းရပ်စ်တန်ပြန်ဆော့ဖ်ဝဲတွေဟာ ကိုယ့်စက်ပစ္စည်းပေါ်က သူခိုးဆော့ဖ်ဝဲတွေကို ရှာမတွေ့တာ မျိုးရှိတတ်ပါတယ်။ အထူးသဖြင့် ဗိုင်းရပ်စ်တန်ပြန်ဆော့ဖ်ဝဲရေးသားသူတွေ မသိတဲ့ သူခိုးဗိုင်းရပ်စ်အသစ်တွေ ဆိုရင် ကာကွယ်ဖို့ပိုခက်ပါတယ်။ ဒါပေမယ့် ဒီလိုအခြေအနေမှာတောင်မှ မိမိစက်ပစ္စည်းမှာ လုံခြုံရေး ကျိုးပေါက်မှု ဆိုင်ရာလက္ခဏာများကို ရှာကြည့်နိုင်ပါတယ်။ လုံခြုံရေးကျိုးပေါက်မှုဆိုင်ရာ လက္ခဏာဆိုတာ သူခိုးဆော့ဖ်ဝဲကူးဆက်ခံထားရရင် ကွန်ပျူတာမှာ ကျန်ခဲ့တတ်တဲ့ သဲလွန်စများကို ဆိုလိုပါတယ်။ ဥပမာ ဝက်ဘ်ကင်မရာမှာရှိတဲ့ မီးဟာ ကိုယ်မဖွင့်ဘဲ သူ့အလိုလိုနေရင်းလင်းနေတာမျိုး မြင်ရနိုင်တယ် (အဆင့်မြင့် သူခိုးဆော့ဖ်ဝဲတွေဆိုရင်တော့ ဝက်ဘ်ကင်မရာမီးကို လှမ်းပိတ်နိုင်စွမ်း ရှိနိုင်ပါတယ်)။ နောက်ဥပမာ တစ်မျိုးကတော့ အစိုးရဦးဆောင်တဲ့ တိုက်ခိုက်မှုတွေနဲ့ ကိုယ့်အကောင့်ကို ပစ်မှတ်ထားတိုက်ခိုက်နေတယ်လို့ သံသယရှိရင် Facebook ၊ Twitter ၊ Microsoft ၊ Google တို့ဟာ သုံးစွဲသူတွေကိုသတိပေးချက်လှမ်းပို့ တာမျိုး လုပ်နိုင်ပါတယ်။

တစ်ချို့ လက္ခဏာတွေကတော့ သိပ်မသိသာပါဘူး။ ကိုယ့်အီးမေးလ်ကို ကိုယ်မသိတဲ့ IP လိပ်စာ ကနေဝင်ကြည့် နေတာမျိုး သို့မဟုတ် ကိုယ့်အီးမေးလ်အားလုံးကို ကိုယ်မသိတဲ့ အီးမေးလ်လိပ်စာနောက်တစ်ခုကို အလို အလျောက်ပေးပို့ဖို့ setting မှာဝင်ရောက်ပြောင်းလဲထားတာမျိုး တွေ လုပ်ထားနိုင်ပါတယ်။ ကိုယ့် အင်တာနက် ကွန်ယက်ကနေ အသွားအလာလုပ်မှုတွေကို စောင့်ကြည့်နိုင်စွမ်းရှိရင် ဒီအသွားအလာတွေရဲ့ အချိန်နဲ့ ပမာဏကို ကြည့်ပြီး လုံခြုံရေးကျိုးပေါက်မှုရှိမရှိ ဆန်းစစ်နိုင်ပါတယ်။ နောက်ထပ်ဥပမာတစ်ခုက ကိုယ့်ကွန်ပျူတာက ထိန်းချုပ်ဆာဗာ တစ်ခုနဲ့ သွားချိတ်နေတာမျိုး ဖြစ်နိုင်ပါတယ်။ ထိန်းချုပ်ဆာဗာဆိုတာ သူခိုးဆော့ဖ်ဝဲကူးဆက် ထားတဲ့စက်ပစ္စည်းတွေ၊ ကူးဆက်ထားတဲ့ စက်ပစ္စည်းကပေးပို့တဲ့ အချက်အလက် တွေကို လက်ခံရရှိတဲ့ အခြား စက်ပစ္စည်းတွေထံ အမိန့်ပေးမှုတွေ လှမ်းပို့နိုင်တဲ့ကွန်ပျူတာတစ်မျိုးကို ဆိုလိုပါတယ်။

ကွန်ပျူတာပေါ်တွင် သူခိုးဆော့ဖ်ဝဲရှာဖွေတွေ့ရှိလျှင် ဘာလုပ်သင့်သနည်း။

ကွန်ပျူတာပေါ်မှာ သူခိုးဆော့ဖ်ဝဲ ရှာတွေ့ခဲ့ရင် အင်တာနက်ဖြတ်ပြီး ကွန်ပျူတာအသုံးပြုမှုကို ချက်ချင်းရပ်ပါ။

ကွန်ပျူတာခလုပ်ခုံပေါ်မှာ နှိပ်သမျှအကြောင်းအရာတွေက တိုက်ခိုက်သူဆီ ရောက်တာမျိုး ဖြစ်နေနိုင်ပါတယ်။ ကွန်ပျူတာကို လုံခြုံရေးဆိုင်ရာ ကျွမ်းကျင်သူ တစ်ဦးဆီယူသွားပြီး သူခိုးဆော့ဖ်ဝဲအကြောင်း ပိုသိလာအောင် စစ်ဆေးကြည့်လို့ရပါတယ်။ သူခိုးဆော့ဖ်ဝဲကိုရှာတွေ့လို့ ဖယ်ရှားလိုက်ပြီဆိုရင်တောင် လုံခြုံမယ်လို့ အာမ မခံနိုင်ပါဘူး။ တစ်ချို့ သူခိုးဆော့ဖ်ဝဲတွေသုံးပြီး တိုက်ခိုက်သူတွေက ကူးဆက်ခံရတဲ့ ကွန်ပျူတာပေါ်မှာ သူတို့ရိုက်ထည့်ချင်တဲ့ ကုဒ် ရိုက်ထည့်လို့ရနိုင်ပါတယ်။ ထို့အပြင် ကိုယ့်ကွန်ပျူတာကို ချုပ်ကိုင်ထားနိုင်ချိန်မှာ အခြားသူခိုးဆော့ဖ်ဝဲတွေကို ထပ်ပြီးမတပ်ဆင်ထားဘူးလို့ မပြောနိုင်ပါဘူး။

လုံခြုံစိတ်ချရတဲ့ အခြားကွန်ပျူတာတစ်ခုကိုသုံးပြီး ကိုယ့်ရဲ့ စကားဝှက်တွေကို ပြောင်းပါ။ သူခိုးဆော့ဖ်ဝဲ ကူးဆက် ခံထားရချိန်မှာ ကိုယ့်ကွန်ပျူတာပေါ်မှာ ရိုက်ထည့်ခဲ့ဖူးတဲ့ စကားဝှက် မှန်သမျှကို ပြန်စဉ်းစားပြီး အသစ်ပြောင်းပါ။

သူခိုးဆော့ဖ်ဝဲကို ဖယ်ရှားဖို့အတွက် ကွန်ပျူတာလည်ပတ်မှုစနစ် ကို ပြန်လည်တပ်ဆင် (reinstall) သင့်ပါတယ်။ ဒီနည်းနဲ့ သူခိုးဆော့ဖ်ဝဲအများစုကို ဖယ်ရှားနိုင်မှာဖြစ်ပေမယ့် တစ်ချို့အဆင့်မြင့်တဲ့ သူခိုးဆော့ဖ်ဝဲတွေတော့ ကျန်နေနိုင်ပါတယ်။ ကိုယ့်ကွန်ပျူတာ ဘယ်တုန်းက သူခိုးဆော့ဖ်ဝဲကူးဆက်ခံရမှန်းသိရင် အဲဒီရက်မတိုင်ခင်က ဖိုင်တွေအကုန်လုံးကို တစ်ခေါက်ပြန်တပ်ဆင်သင့်ပါတယ်။ ကူးဆက်ခံရပြီးသုံးတဲ့ ဖိုင်တွေကို ပြန်လည် တပ်ဆင်ရင် နောက်တစ်ခေါက် ထပ်မံကူးဆက်ခံရနိုင်တာ သတိပြုပါ။