အင်တာနက်ဖြတ်တောက်ချိန်တွင်မှတ်တမ်းတင်ခြင်း

လက်တွေ့ကျသော အကြံပေးချက်များပါဝင်သည့်ဘလော့ဂ်စီးရီး

ရေးသားသူ - Yvonne Ng ပုံပိုးသူ - Arul Prakkash
နောက်ဆုံးပြန်လည်သုံးသပ်သည့်ရက်စွဲ - ဇန်နဝါရီ ၃၀ ရက် ၂၀၂၀ ခုနှစ်
https://wit.to/documenting-shutdowns

၂၀၁၉ဇွန်လမှစ၍မြန်မာနိုင်ငံတွင်လူ့အခွင့်အရေးချိုးဖောက်မှုနှင့်လူသားချင်းစာနာမှုဆိုင်ရာအကြပ်အတည်းပြဿနာများဆက်တိုက်ဖြစ်ပွားလျက်ရှိရာနိုင်ငံပို့ဆောင်ရေးနှင့်ဆက်သွယ်ရေးဝန်ကြီးဌာန၏ ညွှန်ကြားတယ်လီဖုန်းကုမ္ပဏီများ သည် ယင်းတို့၏ မိုဘိုင်းအင်တာနက်ဝန်ဆောင်မှုများကို ရုခိုင်ပြည်နယ်နှင့် အိမ်နီးချင်း ချင်းပြည်နယ်တို့တွင် ဖြတ်တောက်ထားခဲ့သည်။

'ငြိမ်းချမ်းရေး၏အနှောင့်အယှက်များ'နှင့်တရားမဝင်လှုပ်ရှားမှုများ'ဟူ၍ကိုးကားပြီး လူများ၏အကျိုးအတွက် အင်တာနက်ဖြတ်တောက်ခြင်းကို ဥပဒေပြဋ္ဌာန်းသည်ဟု မြန်မာအစိုးရက ပြောဆိုခဲ့သည်။ အဖြစ်မှန်မှာ အင်တာနက်ဖြတ်တောက်ခြင်းကြောင့် လူသန်းပေါင်းများစွာအား မရှိမဖြစ်သော သတင်းအချက်အလက်နှင့် ဆက်သွယ်ရေးကိုအသုံးပြုခွင့်၊လူသားချင်းစာနာမှုဆိုင်ရာကြိုးပမ်းမှုများကိုရပ်တန့်စေခဲ့သည်။

"ထိုကဲ့သို့အင်တာနက်ဖြတ်တောက်ခြင်းသည်ဆက်လက်ဖြစ်ပွားနေသောရိုဟင်ဂျာလူမျိုးတုံးသတ်ဖြတ်မှုနှင့် ရုခိုင်ပြည်နယ်ရှိစစ်ပြစ်မှုကျူးလွန်ခြင်းများအတွက်စစ်သွေးကြွများကိုပစ်မှတ်ထားစေကာမူ အချိုးအစားမညီမျှသော ဖြတ်တောက်ခြင်းသာ ဖြစ်သည်" ဟု Fortify Rights အဖွဲ့မှ Matthew Smith က ဖော်ပြခဲ့သည်။

အင်တာနက်ဖြတ်တောက်ခြင်းအား ၂၀၁၉စက်တင်ဘာလတွင်မြို့နယ်၅မြို့နယ်၌တစိတ်တပိုင်းရှုပ်သိမ်းပေးခဲ့သော်လည်းဆက်လက်ဖြစ်ပွားနေဆဲဖြစ်သည်။ထိုတစ်လတည်းမှာပင်ရိုဟင်ဂျာလူများစုထွက်ပြေးခဲ့သောအိမ်နီးချင်းဘင်္ဂလားဒေ့ရှ်နိုင်ငံတွင်လည်းသက်ဆိုင်ရာအာဏာပိုင်များက3G/4Gservicesများကိုပိတ်ဆို့တားဆီးရန် တယ်လီဖုန်းအော်ပရေတာများကို ညွှန်ကြားခဲ့ပြီး ရိုဟင်ဂျာဒုက္ခသည်စခန်းများတွင် တယ်လီဖုန်း SIM ကဒ်များ ရောင်းချခြင်းကိုရပ်ရန်ညွှန်ကြားခဲ့သည်။ ၂၀၂၀ နှစ်ဆန်းပိုင်းမှစ၍ ရုခိုင်ပြည်နယ် ၄ မြို့နယ်အား ကမ္ဘာနှင့်အဆက်အသွယ်ပြတ်တောက်စေခဲ့ပြီး ဘင်္ဂလားဒေ့ရှ်နိုင်ငံရှိ ဒုက္ခသည်စခန်း များတွင်လည်း ဝန်ဆောင်မှုကို ဆက်လက်၍ကန့်သတ် ထားခဲ့သည်။

အင်တာနက်ဖြတ်တောက်ချိန်တွင် မှတ်တမ်းတင်ခြင်း

အင်တာနက်ဖြတ်တောက်ခြင်းသည်ကမ္ဘာနှင့်အဝှမ်းမြင့်တက်လျက်ရှိသည်။AccessNow's ၏ #keepItOn campaign အရ ၂၀၁၉ ဇန်နဝါရီမှဇူလိုင်လအတွင်း (၁၂၈) ကြိမ်၊၂၀၁၈ တွင်(၁၉၆)ကြိမ် တို့မှာ ၂၀၁၇ တွင်(၁၀၆)ကြိမ်၊ ၂၀၁၆ တွင် (၇၅) ကြိမ်များနှင့် နှိုင်းစာလျှင် သိသာစွာမြင့်တိုး ဖြစ်ပေါ်ခဲ့သည်။ ကမ္ဘာတဝှမ်းတွင် အစိုးရများသည် ဆက်သွယ်ရေးကုမ္ပဏီများနှင့်ပူးပေါင်းပြီး အင်တာနက်ဖြတ်တောက်ခြင်းကို နည်းဗျူဟာတရပ်အနေဖြင့် တိုးမြှင့်ပြုလုပ်ခဲ့ပြီး လူထုအားဖိနှိပ်ခြင်း၊ စည်းရုံးလှုံ့ဆော်ရေးများကို တားဆီးခြင်းနှင့် လူ့အခွင့်အရေးချိုးဖောက်မှု အချက်အလက်များကို မှတ်တမ်းတင်ခြင်းနှင့် မျှဝေခြင်းများကို ရပ်တန့်စေခဲ့သည်။

“အင်တာနက်ဖြတ်တောက်ခြင်းနှင့် လူအခွင့်အရေးချိုးဖောက်မှုများသည် ချိတ်ဆက်မှုရှိရှိဖြစ်ပေါ်နေသည်”

-Berhan Taye, AccessNow

အင်တာနက်ဖြတ်တောက်ခြင်းနည်းပုံစံအမျိုးမျိုးတို့မှာလူကြိုက်များသော ပလက်ဖောင်းအထူးပြုပိတ်ဆို့တားဆီးခြင်းဖြစ်သောရေပန်းစားသောခရာနှင့်ဝက်ဘ်ဆိုက်များကို ပိတ်ပင်တားဆီးခြင်း၊မိုဘိုင်းဒေတာကိုဖြတ်တောက်ခြင်း၊အင်တာနက်မြန်နှုန်းကိုထိန်းချုပ်ခြင်းနှင့် အင်တာနက်ကိုလုံးဝဖြတ်တောက်ခြင်းတို့ပါဝင်သည်။အထက်ပါပိတ်ပင်ခြင်းအားလုံးသည်အချိန်နှင့်တပြေးညီ သတင်းအချက်အလက်များဆက်သွယ်ပို့ဆောင်ခြင်း၊ချိုးဖောက်မှုများကိုဖော်ထုတ်ခြင်းကို အနှောင့်အတားဖြစ်စေသည်။

ထိုအခြေအနေများသည် လူထုဆန္ဒပြခြင်း၊ မဲဆန္ဒပေးခြင်းနှင့် နိုင်ငံရေး မတည်ငြိမ်သည့်အချိန်များတွင် မကြာခဏဖြစ်ပေါ်လေ့ရှိပြီး ပြည်နယ်တွင်း ဖိနှိပ်ခြင်း၊ စစ်တပ်၏ထိုးစစ်နှင့်အကြမ်းဖက်မှုများ မြင့်မားချိန်နှင့် မကြာခဏအတူတကွဖြစ်ပေါ်သည်။အာဏာပိုင်အစိုးရအနေဖြင့်အင်တာနက်ဖြတ်တောက်ခြင်းကို လူထုလုံခြုံရေးသို့မဟုတ်အခြားအကြောင်းပြချက်များရှင်းလင်းဖော်ပြသော်လည်းထိုဖြတ်တောက်ခြင်းမှာ ဖိနှိပ်ခံရသောပြည်နယ်များတွင်ယင်းလူထုအားသတင်းအချက်အလက်နှင့်နိုင်ငံရေးဇာတ်ကြောင်းများ ထိန်းချုပ်နိုင်မှုပျောက်ကွယ်မည်ကိုစိုးရိမ်ကြောင့်ကြသည်မှာထင်ရှားလှပေသည်။အင်တာနက်ဖြတ်တောက်ခြင်း သည်လူ့အခွင့်အရေးချိုးဖောက်ခြင်းဖြစ်ပြီး၊လူအများ၏ဘဝနှင့်ရှင်သန်ရေးကိုဟန့်တားခြင်းနှင့်ကမ္ဘာလုံး ဆိုင်ရာ စီးပွားရေးသက်ရောက်မှုများကိုဖြစ်စေနိုင်သည်။

လူ့အခွင့်အရေးချိုးဖောက်မှုကို မှတ်တမ်းတင်ခြင်းသည် အင်တာနက်ဖြတ်တောက်ထားသည့် အချိန်တွင် ယခင်အခါများထက်ပိုပြီးအရေးပါသည်။

သတင်းအချက်အလက်ကိုချက်ချင်းဝေမျှခွင့်မရသော်လည်းမှတ်တမ်းတင်ထားခြင်းသည်သက်ဆိုင်ရာအားဏာပိုင်များရေငုံနှုတ်ပိတ်ရန်ကြိုးစားမှုအားအသံဖြစ်စေခြင်းနှိပ်စက်ခြင်းများအားသက်သေအဖြစ်လုံခြုံစွာထားရှိပြီးနောင်တချိန်တွင်တာဝန်ယူမှုရှိရန်ပြန်လည်အသုံးချနိုင်သည်။ထိုသို့ဖိနှိပ်နေသောအခြေအနေတွင် အင်တာနက်ဖြတ်တောက်ခြင်းကဲ့သို့စက်ပိုင်းဆိုင်ရာအနှောင့်အတားကြားမှတ်တမ်းတင်ခြင်းနှင့်အချက်အလက်များကို လုံခြုံစွာထိန်းသိမ်းရန်သည် ကျိန်းသေပေါက် အန္တရာယ်ရှိပြီး စွန့်စားရသော စိန်ခေါ်မှုတရပ်ဖြစ်သည်။

တက်ကြွ လှုပ်ရှားသူများသည် အချက်အလက်များကို မှတ်တမ်းတင်ခြင်းနှင့် မီဒီယိုများ ထိန်းသိမ်းခြင်းအပြင် အော့ဖ်လိုင်း(offline)အချိန်တွင် မျှဝေခြင်း ကို မည်ကဲ့သို့ ပိုပြီးလုံခြုံစွာ ပြုလုပ်နိုင်သလဲ?

စီးရီးများ

အင်တာနက်ဖြတ်တောက်ထားချိန်တွင်အတွေ့အကြုံရှိခဲ့သောတက်ကြွလှုပ်ရှားသူများနှင့်ကျွန်ုပ်တို့အတူတူလုပ်ခဲ့သောအလုပ်များမှလေ့လာခဲ့ရသော**“အင်တာနက်ဖြတ်တောက်ချိန်တွင်မီဒီယိုဖမ်းယူပြီးမှတ်တမ်းများကို ထိန်းသိမ်းခြင်း”**အသုံးဝင်သည့်အကြံပေးချက်များနှင့်ချဉ်းကပ်နည်းများကိုဒီစီးရီးတွင်မျှဝေသွားမှာဖြစ်ပါသည်။အင်ဒရိုက်(Android)စက်များအတွက်ရည်စူး၍ရေးသားသော်လည်းအိုင်ဖုန်း(iPhone)တွင်လည်းအသုံးချနိုင်သည်။အချို့နည်းဗျူဟာများသည်ကြိုတင်အစီအစဉ်ချခြင်းနှင့်(အင်တာနက်အသုံးပြုခြင်းများ)လိုအပ်သည်။ထို့ကြောင့်ပြန်လည်သုံးသပ်ခြင်း၊လက်တွေ့အခြေအနေဖြစ်သောအင်တာနက်ဖြတ်တောက်ချိန်တွင်မှတ်တမ်းဖို့လိုအပ်ချိန်မတိုင်မီတဆင့်ချင်းအကောင်အထည်ဖော်ထားသင့်သည်။သင်ခန်းစာများကိုကော်ပီသိမ်းဆည်းထားခြင်းဖြင့်အင်တာနက်ဖြတ်တောက်ချိန်တွင်ပြန်လည်ရည်ညွှန်းခြင်း၊မျှဝေခြင်းများပြုလုပ်နိုင်သည်။

နောက်ဆုံးအနေဖြင့်ထိုနည်းပညာများနှင့်နည်းလမ်းများကိုနေ့စဉ်နေ့တိုင်းလုပ်ငန်းတခုအနေနဲ့ လေ့ကျင့်ခြင်းဖြင့် အကြပ်အတည်းကြုံလာမည့်အချိန်မတိုင်မီတွင် သဘာဝ အလျောက်အလေ့အကျင့်ဖြစ်နေပေလိမ့်မည်။

- ပြင်ဆင်ခြင်း
  ဖုန်းကို အော့ဖ်လိုင်း(offline)နဲ့ မှတ်တမ်းတင်ဖို့ ပြင်ဆင်ထားခြင်း
- အမိဖမ်းယူခြင်း
  ဒီမှတ်တမ်းတင်တဲ့ App ကိုသုံးလို့ရမလား?
- ထိန်းသိမ်းခြင်း
  အင်တာနက်ဖြတ်တောက်ချိန်တွင် ခိုင်လုံအတည်ပြုထားသော မီဒီယာကိုထိန်းသိမ်းခြင်း
  ဖုန်းမီဒီယာကို အင်တာနက် သို့မဟုတ် ကွန်ပျူတာမရှိဘဲ အရန်သိမ်းဆည်း back up ထားခြင်း
- မျှဝေခြင်းနှင့် ဆက်သွယ်ခြင်းအင်တာနက်ဖြတ်တောက်ချိန်တွင် မျှဝေခြင်းနှင့်ဆက်သွယ်ခြင်း

နောက်ဆုံးမှတ်ချက်။အက်တာနက်ဖြတ်တောက်ချိန်များတွင်ထိုအကြံပေးချက်များမှတ်တမ်းတင်နိုင်ရန် အကူအညီဖြစ်စေသော်လည်းအထူးပြုပြောလိုသည်မှာနောက်ဆုံးပိတ်ဖြေရှင်းမှုသည်အင်တာနက်အသုံးပြုခွင့်ကို ပြန်လည်ရရှိရန်၊လူများ၏အခွင့်အရေးဖြစ်သော မှတ်တမ်းတင်ခြင်းကို အောင်မြင်စွာကာကွယ်ရန်၊ လွတ်လပ်စွာပြောဆိုခွင့်သတင်းအချက်အလက်ရရှိခွင့်နှင့်လူစုရုံးခွင့်တို့ဖြစ်သည်။ ကံကောင်းသည်မှာ NetBlocks, AccessNow ကဲ့သို့အဖွဲ့အစည်းတော်တော်များများက ကမ္ဘာလုံးဆိုင်ရာလှုပ်ရှားမှုအနေဖြင့် တက်ကြွစွာစောင့်ကြည့်လေ့လာနေပြီးအင်တာနက်ဖြတ်တောက်ခြင်းသတင်းအချက်အလက်များကိုမျှဝေနေသည်။ကမ္ဘာလုံးဆိုင်ရာထောက်ခံပြောဆိုသူများအနေဖြင့်လည်းအင်တာနက်ဖြတ်တောက်ခြင်းနှင့် ဆန့်ကျင်သောတရားရေးများကိုနည်းဗျူဟာများဆွဲ၍စေ့စပ်ဆွေးနွေးလျက်ရှိသည်။လူ့အခွင့်အရေးခိုင်မာမှုအတွက် ကျွန်ုပ်တို့ကလည်း သူတို့နှင့်တသားတည်း စည်းလုံးစွာရပ်တည်နေသည်။

အော့ဖ်လိုင်း(offline) မှတ်တမ်းတင်ခြင်းအတွက် ဖုန်းကိုပြင်ဆင်(setup)ခြင်း

အင်တာနက်ဖြတ်တောက်ထားသော်လည်း မှတ်တမ်းတင်သူများအနေနှင့် အရေးကြီးဗီဒီယိုများဖမ်းယူနိုင်ပြီး ထိုဗီဒီယိုအထောက်အထားများကို အော့ဖ်လိုင်း(offline) သို့မဟုတ် အွန်လိုင်း(online) ပြန်ရသည့်အချိန်တွင် မျှဝေခြင်း ပြုလုပ်နိုင်သည်။အော့ဖ်လိုင်း(offline)မှတ်တမ်းတင်ခြင်းအတွက်ဖုန်းကိုပြင်ဆင်(setup)ခြင်း အတွက်အသုံးဝင်မည့်အချက်အလက်များကို တက်ကြွလှုပ်ရှားသူများနှင့် အခြားကျင့်သုံးသူများဆီမှ ကျွန်ုပ်တို့ အောက်ပါအတိုင်းလေ့လာခဲ့သည်။သတိပြုရန်မှာ အချို့သောအချက်များသည် **အင်တာနက်အသုံးပြုရန်** လိုအပ်သည်။ ထို့ကြောင့် အင်တာနက်ဖြတ်တောက်ချိန်မတိုင်မီ သို့မဟုတ် အင်တာနက်ပြန်လည်ရရှိချိန်တွင် လုပ်ဆောင်ထားရန်ဖြစ်သည်။ ထပ်မံပြောကြားလိုသည်မှာ ထိုအချက်များကို စိတ်ဖိစီးမှုရှိနေသည့် အချိန်ကျမှ လုပ်ဆောင်ရန်မစောင့်ဆိုင်းပါနှင့်။ ယခုလုပ်ဆောင်ထားပါ။ အကြပ်အတည်း ကျရောက်သည့်အချိန် မတိုင်မီ **ဖုန်းအသုံးပြုခြင်းကိုအချိန်ယူ၍လေ့ကျင့်ထားပါ။**အင်တာနက်ဖြတ်တောက်ချိန်သည်သတင်းအချက်အလက်များကိုတိုးမြှင့်ထိန်းချုပ်ထားသည့်အချိန်သို့မဟုတ်လွတ်လပ်စွာသဘောထားထုတ်ဖော်ခွင့်၊စုရုံးခွင့်များကိုကန့်သတ်ထားသည့်အချိန်များနှင့်တိုက်ဆိုင်နေတတ်သည်။သင်သည်မှတ်တမ်းတင်သူဖြစ်လျှင်မိမိကိုယ်ကိုသော်လည်းကောင်း၊မိမိ၏သတင်းအချက်အလက်များကိုသော်လည်းကောင်းအထူးသတိပြုကာကွယ်ရန်အချိန်ဖြစ်သည်။သက်ဆိုင်ရာအာဏာပိုင်များကသင့်ဖုန်းကိုသိမ်းယူနိုင်ခြေအလားအလာ၊ဖုန်းကိုမဖြစ်မနေunlockလုပ်ခိုင်းနိုင်ခြေ၊အကြောင်းအရာများကိုထုတ်ပြခိုင်းသောအခြေအနေများရှိလျှင်(အင်တာနက်ဖြတ်တောက်ချိန်၊အခြား)မှတ်တမ်းတင်ရန်အတွက်သီးသန့်ဖုန်းတလုံးသုံးရန်စစဉ်းစားပါ။ထိုသို့သုံးစွဲခြင်းဖြင့်မိမိကိုယ်ပိုင်အချက်အလက်များ (contacts, accounts, message, etc) ခိုးယူရရှိခြင်း အခွင့်အလမ်းကို နည်းစေလိမ့်မည်။

ထိုသို့သီးသန့်စက်မသုံးနိုင်လျှင်လည်းယခုနည်းလမ်းများကိုဆက်လက်သုံးစွဲခြင်းဖြင့်လည်း အထိခိုက်မခံနိုင်သောဒေတာများကို ပိုမိုကောင်းမွန်စွာ လုံခြုံစေလိမ့်မည်။

ဖုန်းအဟောင်းကိုရည်ရွယ်ချက်ပြောင်းသုံးစွဲလျှင် ဒေတာအရင်ရှင်းပစ်ပါ

ဒေတာရှင်းရန် factory reset ကို run ပါ

မှတ်ချက်။လေ့လာချက်များအရဖုန်းကိုfactoryresetrunသော်လည်းရှိသမျှဒေတာအားလုံးရှင်းမည်မဟုတ်ပါ ။

အမှန်မှာရာနှုန်းပြည့်လုံခြုံစွာဒေတာများကိုရှင်းလင်းချင်လျှင်ဖုန်းကိုဖျက်ဆီးရမည်။သို့သော်ထိုနည်းလမ်းသည် ဖုန်းကိုပြန်လည်သုံးစွဲချင်လျှင်ရွေးချယ်လို့ရမည့်နည်းလမ်းမဟုတ်ပါ။ယခုဆောင်းပါးတွင်Android အင်ဂျင်နီယာတဦးက အကြံပေးထားသည်မှာ factory reset မလုပ်မီ ဖုန်းထဲရှိအကြောင်းအရာ များကို လျှို့ဝှက်လုံခြုံရန်သေချာစေရမည်။ယခုလက်ရှိဖုန်း အများစုတွင် မူရင်းအားဖြင့် လျှို့ဝှက်လုံခြုံမှုရှိသော်လည်း အကယ်၍မရှိခဲ့လျှင် resetting မလုပ်မီ setting ကိုသွားပါ > security > encrypt လုပ်ပါ။ ထိုနည်းလမ်းသည် သင်factory reset လုပ်ချိန်မှာ encryption key ပျောက်သွားပါက မဖျက်ဆီးရသေးသော ဒေတာများသည်ပင် ဖတ်လို့မရသောအဆင့်သို့ ရောက်သွားမည်။

ဖုန်းလုံခြုံရေးအခြေခံကိုလေ့ကျင့်ခြင်း

အထွေထွေဖုန်းလုံခြုံရေးအလေ့အကျင့်များမှာ အခြေအနေအရပ်ရပ်တွင် အင်တာနက်ဖြတ်တောက်ချိန်ဖြစ်စေ၊ မဖြတ်တောက်ချိန်ဖြစ်စေ အကျုံးဝင်သည်။ အခြားအဖွဲ့အစည်းများ၏ အသုံးဝင်သောအရင်းအမြစ်များ အောက်ပါအတိုင်းဖြစ်သည်။မည်သည့်အရာမှရာနှုန်းပြည့်အာမမခံနိုင်သော်လည်းအချို့အသုံးဝင်သည့်အချက်များပါဝင်သည်မှာ

- သင့်ဖုန်းသည်လျှို့ဝှက်လုံခြုံကြောင်း(encrypted) သေချာပါစေ။ ဖုန်းအသစ်များသည် မူလပင်မကပင် လျှို့ဝှက်လုံခြုံသည် (encrypted)။ မိမိဖုန်း၏လျှို့ဝှက်လုံခြုံမှု မသေချာလျှင် security setting ကို စစ်ဆေးပါ။
- OS (operating system) updates ကို ပုံမှန်စစ်ဆေးပါ။ သူတို့သည် လုံခြုံရေးထိခိုက်နိုင်မှုကို ပြုပြင်နိုင်သည်။
- အရေးကြီးသော app (like message apps) များကို ပုံမှန် update လုပ်ပါ။
- ဖုန်းလျှို့ဝှက်ကုဒ်နံပါတ်ကိုခိုင်မာပါစေ၊ အနည်းဆုံး ဂဏန်းခြောက်လုံးထားပါ၊ လက်ဗွေ မျက်နှာ အမှတ်အသား fingerprint/touch or face ကို အားမကိုးပါနှင့်။
- Screen lock, lock timer ကို set up လုပ်ထားပါ။
- တည်ရှိနေရာ location service ကို (off) မလိုလျှင်ပိတ်ထားပါ။ (emergency location service, location accuracy, location history, location sharing, Wifi, Bluetooth scanning) အကုန်ပါသည်။ အခြားapp တွေမှာရှိသည့် check location permission များလည်းပိတ်ထားပါ။
- Bluetooth နဲ့ Wifi ကိုလည်း မလိုအပ်လျှင်ပိတ်ထားခြင်းဖြင့် device ကို နောက်ယောင်ခံခြင်းမှ ရှောင်ရှားနိုင်သည်။
- ဖုန်းကို မသုံးလျှင် power down ထားပါ။

အသုံးဝင်သောမှတ်တမ်းတင်Appများကို Install လုပ်ခြင်း

ဓာတ်ပုံသို့မဟုတ်ဗီဒီယိုမှတ်တမ်းတင်သောအခါ ဖုန်းထဲရှိ built-in camera app ကို အသုံးပြုနိုင်သည်။ သို့မဟုတ် ပိုပြီးအထူးပြုသောမှတ်တမ်းတင်app (ProofMode သို့မဟုတ် အခြား)များကိုလည်း အသုံးပြုနိုင်သည်။ ထို app များသည် ပိုမိုအားကောင်းသည့် metadata များကို ဖမ်းယူ၊ ပြင်ပသို့ထုတ်ပို့၊ သရုပ်ခွဲ၊ အတည်ပြု၊ လျှို့ဝှက်ထိန်းသိမ်း၊ လုံခြုံသော galleries နှင့် တခြား အဂါရပ်များကို ခွင့်ပြုစေသည်။ အင်တာနက်ဖြတ်တောက်ချိန်ကို မှတ်တမ်းတင်သည့် appဖြစ်သော OONI Probe သည် ပွင့်လင်းအရင်းအမြစ် appဖြစ်ပြီးဖုန်းမှတဆင့်စမ်းသပ်ကာဆိုက်သို့မဟုတ်ပလက်ဖောင်းများကိုပိတ်ဆို့သလားဟုစမ်းသပ်နိုင်သည်။ ထိုစမ်းသပ်မှုမှ ဘယ်လို၊ ဘယ်အချိန်၊ ဘယ်နေရာ၊ ဘယ်သူက ဆိုက်တွေကို ပိတ်ဆို့ထားသလဲ ပြသနိုင်သည်။ဒီ app ကို အသုံးမပြုမီ ဖြစ်နိုင်ခြေရှိသော အန္တရာယ်များကို နားလည်ထားဖို့လိုအပ်သည်။မည်သည့် app ကို အသုံးပြုရမလဲ မသေချာဖြစ်နေပါသလား? ကျွန်ုပ်တို့က လမ်းညွှန်မေးခွန်းများဖြင့် "ဒီမှတ်တမ်းတင်app ကို သင်သုံးသင့်ပါသလား" သင်တန်းတွင်ပံ့ပိုးပေးပါမည်။

နေ့စဉ်အသုံးပြုမည့် App များ Install လုပ်ခြင်း

သင့်ဖုန်းထဲတွင်ဒေတာအနည်းငယ်သာရှိပြီးအထူးပြုသော app များရှိနေခြင်းကြောင့်သံသယဖြစ်ခံရဖွယ်ဖြစ်နိုင်သည်။သင့်ဖုန်းကိုနေ့စဉ်သုံးနေသောdeviceပုံစံပေါ်လွင်စေရန်မိမိမှတ်တမ်းတင်သောနေရာဒေသတွင်အသုံးများသောappများinstallလုပ်ထားပါ(သို့သော် နာမည်ကောင်းရှိသောအရင်းအမြစ်များမှ download) လုပ်ပြီး ဘေးကင်းသောဓာတ်ပုံများကို gallery တွင်ထားပါ။

ဆိုရှယ်မီဒီယာappသုံးလျှင် အခြားနာမည်များနှင့် အကောင့်ဖွင့်လိုက ဖွင့်ထားနိုင်သော်လည်း အကောင့်တုသည် အချို့ပလက်ဖောင်းများ၏ ဝန်ဆောင်မှုစည်းကမ်းကို ဖောက်ဖျက်ရာရောက်သည်။ အချို့ပလက်ဖောင်း
များသည်အကောင့်တုဖွင့်ရန်ခက်ခဲအောင်ကိုယ်ရေးကိုယ်တာအချက်များစိစစ်အတည်ပြုခြင်းလိုအပ်ချက်များထားရှိသည်။ထို့အပြင်အကြောင်းအရာများဖြည့်သွင်းခြင်းသူငယ်ချင်းလက်ခံခြင်း စသည့် လုပ်ငန်းများအတွက် ကြိုးစားအားထုတ်အချိန်သုံးရမည် ဖြစ်သည်။

အင်တာနက်မရှိချိန်တွင် app များ install လုပ်ခြင်း

အင်တာနက်ချိတ်ဆက်ခွင့်မရဘဲ app များကို download and install လုပ်ခြင်းသည် သိသာထင်ရှားသော စိန်ခေါ်မှုဖြစ်သည်။ အင်တာနက်ပြတ်တောက်နိုင်ချေရှိသည်ကို မျှော်မှန်း၍ ကြိုတင်ပြီး download လုပ်ထားရမည်။သင့်အားအထောက်အကူပြုနိုင်သည့် အခြားသောနည်းဗျူဟာမှာ Android Package (.apk) file ကို download and save လုပ်ထားပါ **(ယုံကြည်ရသော အရင်းအမြစ်**, ဥပမာ တီထွင်သူထံမှ တိုက်ရိုက်download) Phone storage or drive မှာ .apk file အနေနဲ့ သိမ်းထားပါ။ ထို APKများကို အော့ဖ်လိုင်း ထားခြင်းသည် အင်တာနက် မရှိသည့်အချိန်တွင် သင်ရော တခြားသူများပါ မျှဝေခြင်းကို ခွင့်ပြုသည်။စမ်းသပ်သုံးစွဲဖို့အခွင့်အလမ်းမရှိသော်လည်း F-Droid app သည် ထို APK အော့ဖ်လိုင်းများနှင့် လဲလှယ်သုံးစွဲနိုင်သည်။သင်ခန်းစာ

ကိုယ်ရေးကိုယ်တာ၊လျှို့ဝှက်၊အထိခိုက်မခံသောသတင်းအချက်အလက်များကိုဖုန်း(device)ထဲမှဖ

ယ်ထုတ်ထားခြင်း

ဖုန်း(device)ကိုမှတ်တမ်းတင်ရုံသက်သက်သာအသုံးပြုရန် ဖယ်သိမ်းထားဖို့ ကြိုးစားပါ။ email, phone calls, message အတွက် ကိုယ်ရေးကိုယ်တာဖြစ်စေ၊ အန္တရာယ်ရှိသွားနိုင်သောတက်ကြွလှုပ်ရှားမှု အဆက်အသွယ်များနှင့်ဖြစ်စေ ဒီဖုန်း(device)ဆက်သွယ်မှု လုပ်ရန် မသုံးပါနှင့်

အကြောင်းအရာများကို မှေးမှိန်သွားစေမည့် features သုံးခြင်း

အကယ်၍ သင့်ဖုန်းကို ရှာဖွေခံရသည့်အခါ သင့်ရည်ရွယ်ချက်ကို သိသာမှု နည်းစေရန် သို့မဟုတ် အကြောင်းအရာများကို တွေ့ရှိဖို့ ခက်ခဲစေရန် ကူညီမှုပေးသည်။ သင့်ဖုန်းကို အပေါ်ယံလျင်မြန်စွာ စစ်ဆေးခြင်းခံရတဲ့အခါ ယခုကဲ့သို့ရှင်းလင်းသည့် နည်းဗျူဟာများကို လုပ်ဆောင်သင့်သည်။

- Launcher app ကို အသုံးပြု၍ app ၏ shortcut နာမည်နဲ့ အိုင်ကွန် များကို ပြောင်းလဲလိုက်ပါ။ (ဥပမာ - Nova Launcher , အခြား app များလည်းရှိသေးသည်) အချို့app တွေရဲ့ သိသာထင်ရှားမှုကို နည်းစေမည်။

- Private Mode (Samsung) or Content Lock (LG) ကဲ့သို့ ဖုန်းနဲ့ တပါတည်းပါလာသော လျှို့ဝှက် feature များကို အထောက်အကူ သုံးနိုင်သည်။

- အချက်အလက်မပါဝင်သောဖိုင်တခုဆောက်၍".nomedia"ဟုအမည်ပေးFolder တခုအောက်တွင်သိမ်းခြင်းဖြင့် gallery ထဲမှာ သင့်မီဒီယာတွေ မပေါ်လာအောင် ကာကွယ်နိုင်သည်။ မှတ်ချက် - အကယ်၍ မီဒီယာတွေ ပေါ်နေဆဲဖြစ်လျှင် gallery cache ကို clear လုပ်ပါ။ ဖုန်း(devices) အားလုံးတွင် တသမတ်တည်း အလုပ်ဖြစ်ချင်မှ ဖြစ်လိမ့်မည်။

- ဖွက်ထားသော folderများ (“.” နှင့်စသောfolder)ကို file manager app သုံး၍ ဖန်တီးပါ။ ဖွက်ထားသော folderများကို manually ဖြစ်စေ၊ Open Camera ကဲ့သို့သော app သုံးပြီးဖြစ်စေ ရှေ့ခြင်းဖြင့် ဘယ်မီဒီယာကို သိမ်းထားလဲ သတ်မှတ်နိုင်သည်။ ဖွက်ထားသောဖိုင်များကို မမြင်စေရန် setting သို့သွား၍ “show hidden files”ကို “turn off” လုပ်ထားကြောင်း သေချာပါစေ။

- Tella or Eyewitness to Atrocities ကဲ့သို့ မှတ်တမ်းတင်ခြင်းကို အထူးပြု app များသည် လျှို့ဝှက်ထိန်းသိမ်းသော encrypted gallery များတွင်း သီးသန့် မှတ်တမ်းတင်ထားနိုင်ပြီး app ကို သုံး၍သာလက်လှမ်းမီနိုင်သောကြောင့်သင့်ဖုန်းကိုရှာဖွေစစ်ဆေးခြင်းခံရသောအခါ သိသာထင်ရှားမှုကို လျော့နည်းစေသည်။ထိုgalleryများတွင်မှတ်တမ်းတင်သောအခါသီးသန့်လျှို့ဝှက်နံပါတ်passcode လိုအပ်ပြီး သင့်ဖုန်း unlocked ဖြစ်သောအချိန်တွင်တောင် လျှို့ဝှက်ထိန်းသိမ်းမှု (encrypted) ဆက်လက်တည်ရှိနေမည်။

အကြောင်းအရာကိုမှေးမှိန်အောင်လုပ်ရာတွင်အရေးကြီးသောမှတ်ချက်အရေးကြီးသောသတိပြုရန်မှာ အထက်ပါနည်းစနစ်များသည်တစုံတယောက်ကလျင်မြန်စွာလှန်လှောချိန်တွင်သာချပစ်ရန်ဖြစ်ပြီး**တစုံတယာ**

က်ကသေချာစွာကြည့်ရှုသည့်အခါတွင် အကြောင်းအရာများကို အကျိုးသက်ရောက်စွာ ဖွက်ထားနိုင်မည်မဟုတ်ပါ။

မှတ်ထားသင့်သည်မှာ အချို့နိုင်ငံများတွင် သင့်ဒေတာများကို လုံခြုံလျှို့ဝှက်ရန်နှင့်ရှင်းလင်းရန်သုံးသော security app များကို ဥပဒေအရ ကန့်သတ်ခြင်း ပြစ်မှုပေးခြင်း ပြုလုပ်နိုင်သည်။ ထို app များကိုအသုံးပြု၍ သင့်ဒေတာများကို အာဏာပိုင်များကို ရယူခြင်းမှာ ကာကွယ်ရန် ရည်ရွယ်ချက်ဖြင့် သက်သေကိုဖျက်ဆီးခြင်း သို့မဟုတ် စုံစမ်းစစ်ဆေးမှုကို ပိတ်ဆို့ခြင်းများ ပြုလုပ်ပါက ရာဇဝတ်မှုအနေဖြင့် ပြစ်ဒဏ်ပေးနိုင်သည်။ ယခုမြေပုံသည် သင့်နိုင်ငံဥပဒေနှင့်ပတ်သက်၍ မေးခွန်းရှိပါက အစပြုလေ့လာနိုင်သည် (ပြည့်စုံသော်လည်း ၂၀၁၇)

အော့ဖ်လိုင်းမျှဝေရန်ပြင်ဆင်ခြင်း

အကြောင်းအရာများကိုဖမ်းယူပြီးသော်လည်းအင်တာနက်မရှိသည့်အခြေအနေတွင်သင့်လုံခြုံရေးအရသော်လည်းကောင်း၊ နေရာလွတ် ရရင်လည်းကောင်း၊ မျှဝေရန်လည်းကောင်း လိုအပ်လာလျှင် မှတ်တမ်းများကို ဖုန်းမှဖယ်ထုတ်ထားသင့်သည်။မှတ်တမ်းများကိုပုံမှန်offloadဖယ်ထုတ်ထားခြင်းဖြင့်သင့်ဖုန်းကိုသိမ်းဆည်းရှာဖွေပြီး unlock လုပ်ခံရလျှင် အချက်အလက်များပေါက်ကြားသွားသော အခြေအနေကို လျော့နည်းစေသည်။

အင်တာနက်မဆက်သွယ်နိုင်သော်လည်း အခြားဖုန်း သို့မဟုတ် Wifi USB drive စသဖြင့် Wifi or Bluetoothနှင့် ချိတ်ဆက်ထားသော deviceများမှ တဆင့် ဆက်သွယ်နိုင်သည်။ သင့်ဖုန်းသည် ပုံမှန်အားဖြင့် app ဆက်သွယ်မှုစနစ်များမှ ဆက်သွယ်ပို့ဆောင်နိုင်စွမ်း ရှိလိမ့်မည်။ အကယ်၍ ထိုနည်းကိုပုံပိုးလျှင် USB on-the-go (OTG) drive သို့မဟုတ် ကွန်နက်တာနှင့် ပလပ်ထိုးပြီး မှတ်တမ်းများကို OTG drive သို့မဟုတ် အခြားdeviceထဲသို့offload(ဖယ်ထုတ်)လုပ်နိုင်သည်။"အင်တာနက်ဖြတ်တောက်ချိန်အတွင်းဖိုင်များမျှဝေခြင်းနှင့်ဆက်သွယ်ခြင်း"သင်ခန်းစာနှင့် "ဗီဒီယိုဖြင့်သက်သေ - နည်းပညာကိရိယာ - ဖိုင်များလွှဲပြောင်းခြင်း" တွင် ထိုနည်းလမ်းများကို အသေးစိတ်ဆွေးနွေးမည်။

အကြပ်အတည်းမကျရောက်မီအခြေအနေတွင်လေ့ကျင့်ခြင်း

ယခုသို့မဟုတ်အင်တာနက်အသုံးပြုခွင့်ရှိချိန်တွင် ဖုန်းအား setup လုပ်ခြင်းနေ့စဉ်အခြေအနေတွင် appများကို စတင်သုံးစွဲလေ့ကျင့်ရန်(လုံခြုံရေးစိုးရိမ်မှုမရှိသောအချိန်)သို့မှသာသုံးစွဲရာတွင်ရင်းနှီးပြီးသက်တောင့်သက်သာရှိစေမည်။မူသေလေ့ကျင့်ရန်ကောင်းမွန်သောအခြေခံဖုန်းလုံခြုံရေးပြုလုပ်ထားပါ။အခြားစိတ်ပူစရာများရှိလာသော အခြေအနေတွင် သဘာဝအလျောက်သုံးစွဲတတ်ရန်နည်းလမ်းဖြစ်သည်။

ဒီမှတ်တမ်းတင် app ကို သုံးသင့်ပါသလား?

ဗီဒီယိုဖမ်းယူရန် မှတ်တမ်းတင်သူများ အသုံးပြုနိုင်သော app များစွာမှာ
ဖုန်းထဲတွင်ပါဝင်သော "Camera App" မှ အစ ပိုမိုအထူးပြုထားသော မှတ်တမ်းတင် app များဖြစ်သည့် "ProofMode, Tella, Eyewitness to Atrocities" အထိရှိသည်။ အချို့ app ၏ အဂါရုပ်များသည် အင်တာနက်ချိတ်ဆက်ခွင့်ကို မှီခိုသည့်အတွက် အင်တာနက်ဖြတ်တောက်ချိန်တွင် ရရှိနိုင်မည်မဟုတ်သည်ကို သတိချပ်သင့်သည်။ဘယ်တိုကျသော app က သင့်အတွက်အသင့်တော်ဆုံးဖြစ်သည်ကို ကျွန်ုပ်တို့ မပြောနိုင်ပါ။ သင့်အခြေအနေ၊ လိုအပ်ချက်၊ အန္တရာယ် တွင် မူတည်သည် (ဒီဘလော့ဂ်ပို့စ်တွင်ကြည့်ပါ - "သင့် အန္တရာယ်နှင့် ခြိမ်းခြောက်မှုကို ဘယ်လိုအကဲဖြတ်မလဲ")။ အန္တရာယ်အကဲဖြတ်မှုလက်ဝယ်ရှိချိန်တွင် ယခုလမ်းညွှန်မေးခွန်းများသည် ဘယ်မှတ်တမ်းတင် app ကို သုံးရင် သင့်အတွက် အကောင်းဆုံးဖြစ်မှာလဲ

ဆိုတာကို သုံးသပ်ပေးသွားမှာပါ။

App တွေကို ဘယ်သူကလုပ်သလဲ? ယုံကြည်ရသလား?

App တွေကို download and install မလုပ်မီ တီထွင်ထားသူကို ယုံကြည်ရသလား ရည်ရွယ်လို့ဖြစ်စေ မရည်ရွယ်ဘဲဖြစ်စေ မိမိအပေါ် အန္တရာယ်ရှိနိုင်လားဆိုတာ စဉ်းစားပါ
ကြည့်ရှုရမည့် အချို့အချက်များမှာ

- Appကိုတီထွင်ထုတ်လုပ်သူသည်နာမည်ကောင်းရသူလား?သူတို့နှင့်သူတို့ရဲ့toolsတွေနဲ့ပတ်သက်ပြီး ကိုယ့်ရဲ့ကွန်ယက်ထဲမှာ ဘာတွေပြောကြသလဲ?
- Appကိုတီထွင်ထုတ်လုပ်သူသည်ထိခိုက်လွယ်သူလား?သူ့ရဲ့အခြေအနေကိုစဉ်းစား၍သူသည်သင့်ဒေတာများကိုအတင်းအကြပ်လက်လွှဲခိုင်းခံရမည့်သူလားအာဏာပိုင်များကနောက်ကွယ်မှာစေခိုင်းခံရသူလား(ဒါမျိုးဖြစ်ဖူးသူလား)။ဘယ်တိုင်းပြည်မှာဒေတာကိုထိန်းသိမ်းတာလဲ
  သူတို့ရဲ့တရားရုံးဥပဒေအဆုံးအဖြတ်က ဘာတွေလဲ
- Appကို တီထွင်သူကပဲ app ကို maintain လုပ်တာလား maintain မလုပ်ထားတဲ့ tools တွေဟာ ခိုးယူခြင်းခံရဖို့အတွက်ခံနိုင်ရည်ရှိလား။ရှာဖွေတွေ့ရှိတဲ့အခါအမြတ်ထုတ်ခံရနိုင်လား app တီထွင်သူရဲ့ ဝက်ဘ်ဆိုက် သို့မဟုတ် app google play page မှာသွားပြီးလေ့လာ၍ “နောက်ဆုံးupdateရက်စွဲ” ကိုကြည့်ပါ။
- Appကိုတီထွင်သူသည်ဘယ်လောက်ခိုင်မာစွာဖွဲ့စည်းထားလဲဒီappကိုရှေရည်တည်တဲ့အောင် ထိန်းသိမ်းထားနိုင်လား
- Appသည်ပွင့်လင်းအရင်းအမြစ်ဖြစ်ရဲ့လား။စိစစ်ရေးကဖွင့်ပေးထားတဲ့appတွေအားများသောအားဖြင့်သူတို့ရဲ့လုံခြုံရေးပြဿနာတွေကိုအမည်တပ်ပြီးဖော်ထုတ်ပြသထားလေ့မရှိပါဘူး။တီထွင်သူသည်appရဲ့လုံခြုံရေးနဲ့ထိရောက်မှုကိုပွင့်လင်းမြင်သာစေပါသလား။
- ဘယ်လိုအားပေးလှုံ့ဆော်မှု၊မက်လုံးတွေကြောင့်ဒီappကိုတီထွင်စေခဲ့သလဲ သူတို့ရဲ့ ယုံကြည်မှုအတွက် ဘယ်လိုလွှမ်းမိုးမှုရှိသလဲ? ဥပမာ သူတို့က မစ်ရှင်တခု အတွက်လား? အကျိုးအမြတ်အတွက်လား? ငွေကြေးထောက်ပံ့သူ တယောက်ကြောင့်က ပံ့ပိုးတာလား?
  ကုန်ကျစရိတ်သည် ယုံကြည်စိတ်ချရမှုကို တိုက်ရိုက်ရည်ညွှန်း ပြသခြင်းမရှိသော်လည်း app ၏ကုန်ကျစရိတ်သည်လည်း ထည့်သွင်းစဉ်းစားရန် အရေးကြီးသည်။အချို့app များ၏လပေးခသို့မဟုတ် ဗီဒီယိုတခုစီ၏ အဖိုးခကြေးငွေသည်မြင့်မားလှသည်။
  App ရွေးချယ်ရန်အတွက် EFF စောင့်ကြည့်လေ့လာရေး ကာကွယ်ရေး လမ်းညွှန်ကို ဒီမှာကြည့်ပါ

ဒီ app ကို ဘယ်နေရာက download လုပ်နိုင်မလဲ?

နာမည်ကောင်းရှိသော app store သို့မဟုတ် websites မှသာ အမြဲတမ်းDownload and install လုပ်ပါ။ သေချာစေ့စပ်စွာ သုတေသနပြု သော်လည်း အချို့ app store များသည် မှားယွင်းစွာ ဖော်ပြထားခြင်းကြောင့် မကောင်း သောရည်ရွယ်ချက်ဖြင့် တရားမဝင်သော အတုအယောင်များကို download လုပ်စေလိမ့်မည်။ ဥပမာ - လွန်ခဲ့သောနှစ်က ဒစ်ဂျစ်တယ်အခွင့်အရေးဆိုင်ရာ အဖွဲ့အစည်းဖြစ်သော SMEX မှ သတိပေးချက်ထုတ်ခဲ့သည်မှာ ဝက်ဘ်ဆိုက်မျိုးစုံနှင့်ပတ်သက်ပြီး အရောင်းမြှင့်တင်ခဲ့သည့် “WhatsApp

Plus” ဟုခေါ်သော app တခုသည် (သတိပြုရန် WhatsApp၏ ထုတ်ကုန်မဟုတ်ပါ) သုံးစွဲသူများ၏ ဒေတာများကို စုဆောင်းပြီး ရောင်းချနိုင်ချေရှိခြင်း သို့မဟုတ် install လုပ်ထားသည့် ဖုန်းများထဲသို့ ခိုးဝင်အချက်အလက်ယူခြင်းလုပ်နိုင်ခွင့်များ ရရှိစေခဲ့သည်ဟု သတိပေးခဲ့သည်။

လုံခြုံရေးကိုသတိထားသော တီထွင်သူများသည် cryptographic keys များ ပံ့ပိုးထားခြင်းဖြင့် သူတို့၏ စစ်မှန်မှုကိုအတည်ပြုနိုင်စေသည်။ထိုသို့သောလက်မှတ်signatureများကိုမည်ကဲ့သို့အတည်ပြုနိုင်ကြောင်းလည်း ထည့်သွင်းရှင်းပြချက်များပါရှိသည်။

ဒေတာကို ဘယ်နေရာမှာ သိမ်းမလဲ?

အချို့မှတ်တမ်းတင်appများသည်သင့်ရဲ့ဖုန်း(device)ထဲတွင်သာဒေတာနဲ့မှတ်တမ်းများကိုသိမ်းဆည်းနိုင်သော်လည်း အချို့တွင် ဒေတာများကို အခြားအရပ်တွင်နှင့် ထိုအရပ်တွင်သာပို့ပေးသိမ်းဆည်းနိုင်သည်။ အခြေအနေများစွာတွင် app ၏ ဒီဇိုင်းနဲ့ ရည်ရွယ်ချက်အရ - ဥပမာ Eyewitness to Atrocities app သည် သင်၏မပြောင်းလဲထားသော ကော်ပီမှတ်တမ်းများကို Lexis Nexis ထိန်းသိမ်းရာဌာနေသို့ ပို့ပေးခြင်းဖြင့် Eyewitness သည် မူရင်း၏ခိုင်မာမှုနှင့် ချုပ်နှောင်ခြင်း၏ကွင်းဆက်ကို အာမခံနိုင်သည်။ သင်၏မီဒီယာကို လျှို့ဝှက်ထိန်းသိမ်းသော encrypted galleryမှ ပြင်ပသို့ထုတ်ပို့ရာသော်လည်း Eyewitness app အတွင်းတွင်သာ ဖြစ်ပြီး ပို့ပြီးချိန်တွင် လုံခြုံသောကာကွယ်မှုရှိမည်။

သင်မှတ်တမ်းတင်ထားသောအချက်အလက်များကိုသင့်ဖုန်း(device)တွင်သိမ်းမလား၊အဝေးထိန်းနေရာတွင်ပို့ပေး၍ (Tella ကို ရွေးချယ်လျှင်) ထိန်းသိမ်းမလားဆိုတာကို သင်ကိုယ်တိုင်ဆုံးဖြတ်နိုင်သည်။ သို့မဟုတ် သင့်မှတ်တမ်းများကိုသုံးစွဲမည့် ပလက်ဖောင်းသို့မဟုတ် ပြင်ပအဖွဲ့အစည်းများဆီပို့ပြီး အသုံးပြုဖို့ ခွင့်ပြုမလားဆိုတာကို ဆုံးဖြတ်ပါ။ အင်တာနက် ဖြတ်တောက်ချိန်တွင် သင်မှတ်တမ်းများကို အင်တာနက်မှတဆင့်ပို့လို့မရ ဆိုသည့်အချက်ကို သတိပြု၍ အနည်းဆုံးယာယီ ထိန်းသိမ်းရန် (အရန်သိမ်းရန်) သိမ်းဖို့ app လိုအပ်မည်။ (ဖုန်းမီဒီယာကို အင်တာနက် သို့မဟုတ် ကွန်ပျူတာမရှိဘဲ အရန်သိမ်းခြင်း)

သင့်ဒေတာတွေကို အဝေးထိန်းနေရာကို ပို့ပေးရာတွင် မည်သည့်နိုင်ငံတွင် သိမ်းဆည်းမည်ကို သတိပြုပါ။ သင့်ဒေတာသည် ထိုနိုင်ငံများတွင် မည်မျှထိခိုက်နိုင်ရည ရှိကြောင်း၊ တရားရုံးမှ ညွှန်ကြားချက်ဖြင့် သို့မဟုတ် အခြားနည်းဖြင့် ထုတ်ယူနိုင်ခြင်းရှိမရှိ ? ထိုနေရာတွင် ဒေတာများပေါက်ကြားလျှင် မည်သို့ အန္တရာယ်ရင်ဆိုင်နိုင်ရသလဲ?

App က သင့်မီဒီယာကို လျှို့ဝှက်ထိန်းသိမ်းမှာလား?

Tella and Eyewitness to Atrocitiesစတဲ့ appတွေက သင့်မှတ်တမ်းတွေ အတွက် လျှို့ဝှက်ထိန်းသိမ်းသိုလှောင်မှုများကို ဖုန်း၏ပင်မgalleryမှ ခွဲ၍ သိမ်းဆည်းနိုင်ရန် ပံ့ပိုးပေးသည်။ ထိုနည်းဖြင့် သင့်မီဒီယာနှင့်

metadata များသည် app ကို လျှို့ဝှက်နံပါတ်နဲ့ သုံးနေသ၍ ဘယ်တော့မှ လျှို့ဝှက်မှု ပေါက်ကြားမည်မဟုတ်။ ဆိုလိုသည်မှာဖုန်းသည် unlock ဖြစ်သွားသည့်တိုင် မှတ်တမ်းများသည် လျှို့ဝှက်ထိန်းသိမ်းထားရှိမည်။ထိုနည်းလမ်းဖြင့်သင့်မှတ်တမ်းများကို အပိုအဆင့်ကာကွယ်ထားမည်ဖြစ်သည်။

ထိုappသည်အင်တာနက်ပြန်လည်ရရှိပြီးနောက်သင့်မီဒီယာများကိုအဝေးထိန်းနေရာသို့ပို့ဆောင်သိမ်းဆည်းသည့်အခါ လမ်းတွင်တဆင့်နားချိန်၌ မီဒီယာများသည် လျှို့ဝှက်ထိန်းသိမ်းရန် လိုအပ်ချက်ရှိမရှိ စဉ်းစားပါ (ဥပမာ - EyeWitness app)လျှို့ဝှက်ထိန်းသိမ်းခြင်း encryption သည် တချို့နိုင်ငံများတွင် တရားဝင်ဖြစ်ပြီးတချို့နိုင်ငံများတွင် ကန်သန့်ချက် သို့မဟုတ် သုံးစွဲခြင်းကြောင့် ရာဇဝတ်မှု မြောက်နိုင်သည်။

အရေးကြီးသောmetadataများကိုအင်တာနက်မရှိဘဲappကနေ ဖမ်းယူထားနိုင်ပါသလား?

Metadataဆိုသည်မှာသင့်မီဒီယိုသို့မဟုတ်ဓာတ်ပုံများကိုအချိန်နေရာနှင့်အရပ်ဒေသညွှန်ပြသော ဒေတာဖြစ်သည်။ ထိုသတင်းအချက်အလက်များသည် သင့်မီဒီယိုနှင့် ဓာတ်ပုံများကို ဖြစ်ရပ်တခုအတွက် မှတ်တမ်းတင်ရာတွင်ခွဲခြားသတ်မှတ်ခြင်း၊နားလည်စေခြင်း၊စစ်မှန်ကြောင်းသက်သေပြခြင်းနှင့်အတည်ပြုခြင်းများအတွက်တန်ဖိုးရှိသည်။အင်တာနက်ဖြတ်တောက်ချိန်အခြေအနေမျိုးတွင်ထိုapp၏အလိုအလျောက်စုဆောင်းသွားခြင်းသို့မဟုတ်ရှင်းပြချက်များကိုလွယ်ကူစွာထည့်သွင်းနိုင်ခြင်းကြောင့်metadataများသည်လွန်စွာအသုံးဝင်သည်။အဘယ်ကြောင့်ဆိုသော်တစုံတယောက်နဲ့သင်မျှဝေနိုင်သောအချိန်မတိုင်မီ(အသေးစိတ်ဖြစ်ရပ်များသည်မေ့လျော့နိုင်ခြင်းအခြေအနေအရပ်ရပ်ပြောင်းလဲခြင်းတို့ကြောင့်ဖြစ်သည်။

ProofMode ကဲ့သို့သော အထူးပြုထားသည့် app များတွင် ပိုမိုကောင်းမွန်သော metadata features ပါနိုင်ပြီး built-in camera ထက် metadata များကို ပိုပြီးစုဆောင်းနိုင်သည်။ ပိုမိုကောင်းမွန်သော metadata တွင် အမျိုးမျိုးသော ဆင်ဆာဒေတာ၊ အနီးတဝိုက်ရှိ wifi or Bluetooth အချက်များ ဖုန်း(device)၏ ဒေတာ cryptographic hash နှင့် သုံးစွဲသူထည့်သွင်းထားသော အချက်အလက်များ အားလုံးကို မီဒီယာတွင် စစ်မှန်ကြောင်းသက်သေပြခြင်းနှင့် အတည်ပြုခြင်းများ ပါဝင်သည်။

သတိပြုရန်မှာအင်တာနက်ဖြတ်တောက်ချိန်တွင်metadataထုတ်လုပ်နှင့် ရိုက်ကူးရန်အတွက် ဒေတာမလိုသော app ကို သုံးရမည်။အချို့ app များသည် metadata များကို စုဆောင်းရန် hardware ဆင်ဆာအစားအင်တာနက်ကို အားကိုးရခြင်းဖြစ်နိုင်ချေရှိသည်။ဥပမာ - ဒေတာ၏အရပ်ဒေသကို ဖုန်း (device)၏ စောင့်ကြည့်များမှ ဖမ်းယူသည့်အခါ metadata သည် hardware ၏ တကယ့်ရှိနေသော အနေအထား အစားဖုန်း(device)၏ ဒေတာနောက်ဆုံးရခဲ့သည်နေရာကို ရောင်ပြန်ဟပ်သည်။ ဒီ app သည် metadata များကိုထိုနေရာတွင်ပင် အင်တာနက်မရဘဲ သိုလှောင်ထားပေးပြီး မည်သည့်ပုံစံဖြင့်ဖြည့်သည်ဖြစ်စေ စုဆောင်းထားပေးမည် (ဥပမာ - Tell ၏ အော့ဖ်လိုင်းပုံစံ)

App က ဒေတာတွေကို ပြင်ပသို့ ထုတ်ပို့လို့ရသလား?

သင့်ရဲ့ မှတ်တမ်းတင်ချင်တဲ့ရည်ရွယ်ချက်ပေါ်မူတည်ပြီးတော့ ဗီဒီယိုမှတ်တမ်းနဲ့ သူ့ရဲ့metadataတွေကို

ပြင်ပသို့ထုတ်ပို့နိုင်စွမ်းဟာ မရှိမဖြစ်လိုအပ်ပါတယ်။ သူရဲ့ format ဟာ app မှာပဲ ပိုင်ဆိုင်တာမဟုတ်ဘဲ တခြားသူတွေ ဖွင့်လို့ မြင်လို့ သုံးလို့ရတဲ့အခြေအနေဖြစ်ဖို့လိုပါတယ်။ပြင်ပသို့ထုတ်ပို့နိုင်စွမ်းဆိုတာ သင်ရော တခြားသူများရောဟာ app တခုတည်း သို့မဟုတ် ဝန်ဆောင်မှုတခုတည်းကို သုံးတာမဟုတ်ဘဲ အကြောင်းအရာတွေကို လွတ်လပ်စွာ နောက်ထပ်တဆင့်ထပ်ပြီး ဖြန့်ဖြူးနိုင်ဖို့လိုပါတယ်။ သတိပြုရန်မှာ တချို့metadata တွေဟာ certain databases ထဲကိုဝင်လို့မရရင် ဇယားတွေကို နံပါတ်အဖြစ် လွဲပြောင်းလို့မရရင် နားလည်အောင် ဘာသာပြန်ထုတ်ဖော်အသုံးပြုလို့ မရပါဘူး (ဥပမာ - ဆဲလ်တာဝါတိုင်နံပါတ် သို့မဟုတ် wifi ကွန်ယက်)သတိပြုရန်မှာ အချို့ app တွေကျတော့ ကွင်းဆက်အပိတ်ထိန်းထားတာ ဖြစ်နေလို့ အပြင်ကိုထုတ်ပို့ခွင့်မရှိပါဘူး၊ အချို့app တွေကတော့ အပြင်ထုတ်ပို့ဖို့အတွက်ကို ဒီဇိုင်းမလုပ်ထားတာပါ။ တချို့ app တွေက (Eyewitness to Atrocities) မီဒီယာကို ရီမုတ်ဆာဗာဆီ မတင်ဘဲ အပြင်ထုတ်ပို့ခွင့်မပေးပါဘူး (အင်တာနက်သုံးဖို့လိုပါတယ်)
တချို့Appကမီဒီယာတွေအပြင်ထုတ်ပို့လို့ရပြီးတခြားmetadataတွေပို့လို့မရပါ(ဖိုင်ထဲမှာသက်ရှိနေတဲ့meta dataမှအပ)သင့်အနေနဲ့ပြင်ပထုတ်ပို့ဖို့လိုအပ်လာရင်သင်သုံးတဲ့appကမီဒီယာကော်ပီကိုသာပြောင်းလဲခြင်းမရှိဘဲ၊ metadataကော်ပီကိုလည်း ဖတ်လို့ရတဲ့စာသားပုံစံနဲ့သာ ပို့ဖို့ခွင့်ပြုတဲ့ app ဖြစ်ရပါမယ်။
ဥပမာ Tella metadata ဆိုရင် Tella gallery ထဲမှာ လျှို့ဝှက်ထိန်းသိမ်းထားတာဖြစ်ပြီး ပြင်ပကိုထုတ်ပို့တဲ့အခါမှာ CSV အနေနဲ့ ထုတ်ပို့လို့ရပါတယ်။ ဒါ့အပြင် အင်တာနက်ဖြတ်တောက်ချိန်မှာ ပြင်ပထုတ်ပို့ဖို့အတွက် ရွေးချယ်ရန်နည်းလမ်းတွေဖြစ်တဲ့ offline apps သို့မဟုတ် အင်တာနက်ကိုမမှီခိုတဲ့ ဝန်ဆောင်မှုဖြစ်ဖို့လိုအပ်ပါတယ်။ များသောအားဖြင့် app အများစုဟာ ပြင်ပကိုထုတ်ပို့ဖို့အတွက် “share” ဆိုတဲ့ခလုတ်နှိပ်ရင် မျှဝေနိုင်အောင် Android မှာဆိုရင် app စာရင်းတွေထားပြီး ဒီလိုအကြောင်းအရာမျိုးကို ကိုင်တွယ်နိုင်အောင် စုစည်းထားပါတယ်၊ ကံမကောင်းတာတခုကတော့ တီထွင်သူဟာ share menu ကို သူ့စိတ်ကြိုက်လုပ်နိုင်တဲ့အတွက် app တခုနဲ့တခုကြားမှာ တသမတ်တည်းမဖြစ်တတ်ပါဘူး။
အရေအတွက်များတဲ့ဖိုင်အတွက်ဆိုရင် app database မှာသိမ်းထားတဲ့ metadata တွေကို ဝင်ပြီးသုံးလို့မရသော်လည်း သိမ်းထားတဲ့ဖိုင်တွေကို ဖိုင်မန်နေဂျာ app ကနေတဆင့် ဝင်ပြီးသုံးမယ် ကူးယူမယ်ဆိုရင် ပိုပြီးထိရောက်မှုရှိပါတယ်။ ဒီရွေးချယ်မှုနည်းလမ်းဟာ သူတို့ရဲ့ကိုယ်ပိုင်လုံခြုံသော gallery တွေပံ့ပိုးထားတဲ့ app တွေအတွက် ရမှာမဟုတ်ပါဘူး၊ ဘာကြောင့်လဲဆိုတော့ အဲဒီဖိုင်တွေဟာ သိုလှောင်နေရာ (storage) ထဲမှာပဲ လျှို့ဝှက်ထိန်းသိမ်းထားလို့ဖြစ်ပါတယ်။အဲဒီ app တွေဟာဆိုရင် app အတွင်းမှာ sharing function ရှိဖို့လိုအပ်ပါတယ်။

ခိုင်လုံသောမီဒီယာ အချက်အလက်များကိုအင်တာနက်ဖြတ်တောက်ချိန်တွင်ထိန်းသိမ်းခြင်း

လူ့အခွင့်အရေးကာကွယ်သူများ၊ စုံစမ်းစစ်ဆေးသူများ၊ သုတေသနပြုသူများနှင့် သတင်းထောက်များသည် မျက်မြင်သက်သေများက ရိုက်ကူးထားသော ဦးဆုံးလက်မှတ်တမ်းများကိုအားကိုးပြီးမှ လေ့လာစောင့်ကြည့်၊ အစီရင်ခံ၊ လူ့အခွင့်အရေး ချိုးဖောက်မှုများကို အမည်တပ်ခြင်း ပြုလုပ်ရသည်။ ထိုသူများက မှန်ကန်သော အချက်အလက်များပေါ်တွင် ဆောင်ရွက်ကြောင်း သေချာအောင် သုံးစွဲသူများသည် အဆင့်များစွာ လုပ်ဆောင်၍ သူတို့ရရှိသော မှတ်တမ်းများကို စစ်မှန်ကြောင်းအတည်ပြုသည့် ဆောင်ရွက်ချက်သည် အချိန်ကြာမြင့်နိုင်သည်။မှတ်တမ်းတင်သူတယောက်အနေဖြင့် အခြားသူများက သင့်မှတ်တမ်းကို အတည်ပြုပြီးဆောင်ရွက်နိုင်ရန် ရိုးရှင်းသော အချက်တချို့ လုပ်ဆောင်နိုင်သည်။ သို့မှသာ

ထိုမှတ်တမ်းများသည် အချိန်မီ ထိရောက်စွာ အသုံးပြုနိုင်မည်။အောက်ပါ အပိုအချက်များသည် အင်တာနက်ဖြတ်တောက်ချိန်တွင် ပိုပြီးတန်ဖိုးရှိသောကြောင့် ထည့်သွင်းစဉ်းစားသင့်သည်။

- ချက်ချင်းuploadမလုပ်နိုင်သေးရင်ထုတ်လုပ်သောရက်နဲ့နေရာကိုဆိုရှယ်မီဒီယာတွင်တင်ထားခြင်းသည် ရိုက်ကူးထားသော ဗီဒီယိုတွင်ပြသနေသော ရက်တခုအချိန်တခုဒေသတခုရှေ့တွင် ပြသခြင်းသည် အထောက်အကူမဖြစ်ပါ
- တခြားသူupload မလုပ်နိုင်ရင်လည်း မှတ်တမ်းရရှိနိုင်ချေအလုံးစုံ နည်းပါးသည့်အတွက် သင့်ဗီဒီယိုနဲ့ အတည်ပြုနိုင်သည်။
- အော်ဖ်လိုင်းကနေလူများကတဆင့်ဖြတ်ပြီးသင့်ဗီဒီယိုကိုပို့ရမယ်ဆိုရင်ဗီဒီယိုရဲ့ပင်မရင်းမြစ်ကိုခြေရာခံဖို့ခက်ပါသည်။
- လုံခြုံရေးတင်းကြပ်လို့နေရာလွတ်မကျန်လို့အရန်ကူးစရာမရှိလို့အော်ရီဂျင်နယ်ဗီဒီယိုကိုဖုန်းကနေဖျက်ပစ်ဖို့ လိုအပ်မယ်ဆိုရင်၊ ဖုန်းကိုလွှင့်ပစ်ရမယ်ဆိုရင် အဲဒီဗီဒီယိုရဲ့စစ်မှန်မှုကို အာမခံဖို့ ခက်မယ်။

  - ဗီဒီယိုတခုရဲ့ အသေးစိတ်အချက်တွေကို မေ့သွားပြီး app ကလည်း မဖမ်းယူထားဘူးဆိုရင် metadataကိုအင်တာနက်မသုံးဘဲဖမ်းယူထားတယ်ဆိုရင်အဲဒါကိုနောက်ပိုင်းမှသူများတွေက သတ်မှတ်ဖော်ထုတ်လို့ရမှာမဟုတ်ပါ။

အောက်ပါအသုံးဝင်မည့်အချက်အလက်များက“အင်တာနက်ဖြတ်တောက်ချိန်တွင်ခိုင်လုံသောမီဒီယာအချက်အလက်များကိုထိန်းသိမ်းခြင်း”ကိုကူညီပြီးနောက်ပိုင်းမှာမှတ်တမ်းတွေကိုအတည်ပြုခြင်းအသုံးပြုခြင်းကို အကျယ်ချဲ့နိုင်ပါမယ်။

အသေးစိတ်အချက်အလက်များကို ဗီဒီယိုတွင် ထုတ်ဖော်ခြင်းရိုက်ကူးခြင်း

သင့်ဗီဒီယိုတွင် အသေးစိတ်အချက်အလက်များပါဝင်စေခြင်းဖြင့် နောင်အခါ စုံစမ်းထောက်လှမ်းသူသို့မဟုတ် သတင်းထောက်မှ အချိန်နေရာစသဖြင့် ထုတ်ဖော်ဖို့လွယ်ကူနိုင်ရန် သိသာသော မြေပြင်အမှတ်အသား၊ လမ်းအမှတ်အသား၊ လိုင်စင်နံပါတ်ပြား၊ အလံ၊ တိုင်ကပ်နာရီ၊ သတင်းစာ၏ ပထမမျက်နှာ စသည့်အချက်အလက်များပါအောင်ရိုက်ကူးသင့်သည်။သင့်ရဲ့နာမည်နှင့်ဆက်သွယ်ရန်အချက်အလက်များ(အန္တရာယ်ကင်းသည်ဆို)အချိန်၊ရက်စွဲ၊နေရာ၊GPSနဲ့ကိုက်ညီပြောဆိုထည့်သွင်းခြင်းသို့မဟုတ်(စာရွက်ပေါ်တွင်ချရေး၍စာရွက်ကိုထည့်သွင်းရိုက်ကူးခြင်း)ပြုပါ။အသေးစိတ်အချက်အလက်များများပါလေနောက်ပိုင်းတွင်(သင့်ကိုမသိဗီဒီယိုဘယ်နေရာကလာမှန်းမသိသော်လည်း)သုတေသနလုပ်ပြီးအတည်ပြုရန် တစုံတယောက်အတွက် လွယ်ကူလေဖြစ်သည်။“ရိုက်ကူးခြင်းထိန်းသိမ်းခြင်းမျှခြင်းအတွက်အခြေခံအလေ့အကျင့်များ” တွင် ကြည့်ပါ။

Metadata/ဖော်ပြချက်များထည့်သွင်းရန်

မှတ်တမ်းတင်သော အထူးပြုထားသော app များထဲမှ တခု ရဲ့ အခွင့်ကောင်းယူအသုံးချခြင်းဖြင့် ပိုကောင်းမွန်သော metadata သို့မဟုတ် စက်ပိုင်းဆိုင်ရာသတင်းအချက်အလက်များကို ဖုန်းမှ ဆွဲထုတ်ခြင်းနှင့် အခြားသော အပိုဖော်ပြချက်အချက်အလက်များကို ထည့်သွင်းခွင့်ရရှိသည်။ သတိပြုရန်မှာ အင်တာနက်ပိတ်ထားချိန်တွင် အင်တာနက် သုံးစရာ မလိုသော app ဖြင့် မှတ်တမ်းတင်ရိုက်ကူးရန်နှင့် အချက်အလက်များအား ထိန်းသိမ်းရန်ဖြစ်သည်။ သင့်တော်သောappကို ဘယ်လိုရွေးချယ်မလဲ ဆိုတာကို “ဒီမှတ်တမ်းတင်appကိုအသုံးပြုသင့်ပါသလား” တွင်ကြည့်ပါ။

ProofMode ကိုသုံး၍ အချို့သော metadataများကို ဖမ်းယူခြင်း အထူးပြုထားသောမှတ်တမ်းတင်appကို အသုံးမပြုသော်လည်း ဖြည့်စွက်အချက်အလက်များကို ဖန်တီးပြီး မှတ်ချက် မြေပုံ ဓာတ်ပုံများကို ဖုန်းတွင်ထည့်သွင်းနိုင်သည်။အနှစ်သက်ဆုံးဖိုင်မန်နေဂျာappကိုသုံးကာသင့်ဗီဒီယိုထဲရှိဖြည့်ပေါင်းအချက်အလက်များကို စုစည်းထိန်းသိမ်းနိုင်သည် အဓိကကျသော ဖြည့်စွက်အချက်အလက်မှာ အချိန် ရက်စွဲ ရိုက်ကူးထားသောဖြစ်ရပ်တည်ရှိရာနေရာနှင့်တကွရိုက်ကူးသည့်အရင်းအမြစ်(ရိုက်ကူးသူ၏နာမည်နဲ့ဆက်သွယ်ရန် အချက်အလက်များ) ထည့်သွင်းနိုင်သည်။ ထိုအချက်metadata များကို ဗီဒီယိုထဲထည့်သွင်းခြင်း (အားလုံးကိုfolderထဲထည့် zipped) လုပ်ပြီး ထုတ်ပို့ခြင်းဖြင့်မျှဝေနိုင်သည်။

အရန်သိမ်းထားခြင်း back up

ဖုန်းထဲရှိမီဒီယာများကိုbackupအရန်သိမ်းခြင်းပုံမှန်လုပ်ပါ။ သီးသန့် storageနှစ်ခုခွဲထားပါ။ ဥပမာ - On-the-Go(OTG)သို့မဟုတ်wireless thumbdriveကိုဖုန်းနဲ့ချိတ်ဆက်ပြီးကွန်ပျူတာမပါဘဲဆက်နိုင်သည်။ "ဖုန်းမီဒီယာများကိုအင်တာနက်သို့မဟုတ်ကွန်ပျူတာမပါဘဲbackupအရန်သိမ်းခြင်း"တွင် အသေးစိတ်ကြည့်ပါ။ အရန်သိမ်းခြင်းဖြင့် ဖုန်းပျောက်သွား ပျက်သွားခဲ့သော် သင့်တွင်ဗီဒီယိုကော်ပီတခုလက်ကျန် ရှိနိုင်ကြောင်း သေချာစေလိမ့်မည်။အော်ရီဂျင်နယ်ဗီဒီယို၏ စိတ်ချရသော ကော်ပီရှိခြင်းသည် သင့်ဗီဒီယိုကို တခြားနည်းလမ်းမှမြင်သော စုံစမ်းထောက်လှမ်းသူ သို့မဟုတ် သတင်းထောက်က နောက်ပိုင်းတွင် သင့်ထံမှ တိုက်ရိုက်လာယူရန် ထောက်ကူသည်။ (သင့်ကိုနောက်ယောင်ခံလိုက်လာလို့ရတယ်ဆိုပါစို့)၊ တိုပြီးပြည့်စုံသောကွင်းဆက်ကို ဖန်တီးနိုင်လာမည်။

ဖုန်းမီဒီယာများကိုအင်တာနက်သို့မဟုတ်ကွန်ပျူတာမပါဘဲbackup အရန်သိမ်းခြင်း

အရန်သိမ်းဆည်းခြင်းသည် အချက်အလက်တွေ မှတ်တမ်းတွေကို အခန့်မသင့်ဖျက်မိတာ၊ ဖျက်ဆီးမိတာ သင့်ဖုန်းသိမ်းဆည်းခံရတဲ့အခါပြောက်တာတွေမဖြစ်အောင်သေချာစေတဲ့နည်းပါ။အင်တာနက်ပိတ်သွားတဲ့အချိန်၊နှေးသွားတဲ့အချိန်မှာနောက်ခံသိမ်းဆည်းတဲ့အလုပ်ကိုပုံမှန်မလုပ်နိုင်တာတို့သင့်မှတ်တမ်းကို လုံခြုံတဲ့နေရာကိုမပို့နိုင်တာတို့ဖြစ်နိုင်ပါသည်။ဒက်စတော့သို့မဟုတ်လက်တော့ကွန်ပျူတာထဲထည့်ချလိုက်တာလည်းတနည်းအားဖြင့်အရန်သိမ်းနည်းတမျိုးဖြစ်သည်သို့သော်လူတိုင်းမှာတော့ရှိမှာမဟုတ်လို့အောက်ပါရွေးချယ်ခွင့်လမ်းများနဲ့ အသုံးဝင်သော အချက်များသည် ဖုန်းထဲမှာရှိတဲ့ ဖိုင်တွေကို အင်တာနက်ပိတ်သွားတဲ့အချိန် ကွန်ပျူတာမရှိတဲ့အချိန်မှာ အရန်ခံသိမ်းနည်းတခုပဲ ဖြစ်ပါသည်။

OTG or wireless thumb drive အသုံးပြုခြင်း

OTG or wireless thumb drive များသည် USG drive ဖြစ်ပြီး Andriod (အားလုံးမဟုတ်သော်လည်း) တော်တော်များများနဲ့ compatible ဖြစ်သည်OTG thumb drive ကိုဖုန်းနဲ့တိုက်ရိုက်ပလပ်ထိုးပြီးဖြစ်စေ OTG-to-USB adapter သုံးပြီးဖြစ်စေ OTG နဲ့ ဆက်ခြင်းဖြင့် drive ကို ဖုန်းကနေ အားသွင်းနိုင်သည်။ ရေပန်းစားသော OTG driveများမှာ Sandisk, Kingston, Samsung တို့ဖြစ်ပြီး အခြားအမျိုးပေါင်းများစွာလည်းရှိသည်။သိမ်းဆည်းနိုင်သော storage capacity ပေါ်မူတည်ပြီး တခုကို $ 8-25 ကုန်ကျနိုင်သည်။ဖုန်းထဲကမီဒီယာဖိုင်တွေ (backup)အရန်သိမ်းဆည်းဖို့ OTG driveသုံးပြုခြင်း ကြိုးမဲ့ thumb drive / hard drives တွေဟာ ကြိုးမလိုတာကလွဲရင် အခြားပုံမှန် hard drive တွေနဲ့ အတူတူဖြစ်သည်။ ဖုန်းကဲ့သို့ Hard drive နဲ့ ပုံမှန်အားဖြင့် ဆက်လို့မရတဲ့ ဖုန်း(device) တွေကို

ဆက်သွယ်လို့ရအောင် ခွင့်ပြုမှာဖြစ်သည်။ ကြိုးမဲ့drive မှာ OTG drive ထက် အားသာချက် ကတော့ သုံးစွဲသူများစွာကို wireless drive တခုတည်းကနေ တပြိုင်နက်တည်း ဆက်နိုင်တာဖြစ်သည်။ ဘယ်အချိန်မှာအသုံးဝင်လဲဆိုရင် ဆန္ဒပြမှုများဖြစ်နေချိန်မှာ အဖွဲ့လိုက်ရိုက်ကူးမှတ်တမ်းတင်တဲ့အခါမှာ တယောက်ချင်းစီရဲ့ ဗီဒီယိုဖိုင်တွေကို တခြားတယောက်သယ်ဆောင်ထားတဲ့ hard drive ထဲမှာ backup အရန်သိမ်းဆည်းလို့ရနိုင်သည်။ ဖုန်းdevice ကနေ ပါဝါကိုမဆွဲတဲ့အတွက်ကြောင့် ကြိုးမဲ့ drive တွေက ဘတ်ထရီကို သုံးပြီး အားပြန်သွင်းဖို့လိုအပ်တယ်ဆိုတာ မှတ်ထားရမည်ဖြစ်သည်။ တခြားအမျိုးအစားတွေ အများကြီးရှိသော်လည်း SanDisk ကတော့ လူကြိုက်အများဆုံး ကြိုးမဲ့ thumb drive ဖြစ်သည်။ ကြိုးမဲ့ thumb drives တွေက OTG drives တွေထက် ဈေးပိုများပါတယ်။ သိမ်းဆည်းနိုင်သော storage capacity ပေါ်မူတည်ပြီး $ 25-100 ကုန်ကျနိုင်သည်။ ပိုပြီးကြီးတဲ့ အပြင်ပ hard drive တွေကတော့ သိမ်းဆည်းနိုင်သော storage capacity ပေါ်မူတည်ပြီး $ 150 လောက်ကုန်ကျနိုင်ပါသည်။ကြိုးမဲ့ thumb drive ကိုသုံးပြီး ဖုန်းdeviceထဲက မီဒီယာဖိုင်များကို backup အရန်သိမ်းဆည်းခြင်း။

အပြောင်းအလဲ- မသုံးတော့သောဖုန်းအဟောင်းများကိုသုံးခြင်း

OTG သို့မဟုတ် wireless drive မရှိဘူးဆိုရင် မသုံးတော့တဲ့ ဖုန်းအဟောင်း တွေကိုလည်း backup အရန်သိမ်းဆည်းဖို့အတွက် ရည်ရွယ်ချက်ပြောင်း သုံးနိုင်ပါသည်။ ဖုန်းနှစ်ခုနီးကပ်သောအကွာအဝေးရှိရင် Bluetooth, Wifi Direct သို့မဟုတ် NFCအနီးကပ်ဆက်သွယ်မှုစနစ်၊ အင်ဒရိုက်ဘီန်း ဆက်သွယ်မှုစနစ်Andriod Beam ဆက်သွယ်ပြီး မီဒီယာတွေကို ကော်ပီလုပ်လို့ရပါသည်။Bluetooth or Wifi Direct တွေက ကြိုးမဲ့စနစ်ဖြစ်ပြီး ကွန်ယက်ဖြန့်ခွဲမှု သို့မဟုတ် ဆက်သွယ်မှုစုံရပ် မရှိဘဲ စက်နှစ်ခုကို “စုံတွဲဆက်သွယ်”နိုင်ပါသည်။Wifi Direct ကတော့ Bluetooth ထက်စာရင် ဝေးဝေးရောက်ပြီး ဒေတာတွေကို
မြန်မြန်ပြောင်းလွှေ့နိုင်စွမ်းရှိပေမယ့်ပါဝါသုံးတာအရမ်းများပါသည်>တချိန်တည်းမှာNFCအနီးကပ်ဆက်သွယ်မှု (~၄စင်တီမီတာ)နှင့်ပိုပြီးနီးနီးအကွာအဝေးမှာရှိပြီးပြောင်းလွှေ့ချိန်လည်းပိုနှေးကွေးပါသည်။သို့သော်သူက ဆက်သွယ်မှုပိုမြန်ပြီးပါဝါသုံးတာပိုနည်းတာမို့ခပ်မြန်မြန်နဲ့နည်းနည်းပဲပြောင်းလွှေ့သည်။စက်နှစ်ခုလုံးလက်ထဲမှာ ရှိမယ်ဆို အသုံးဝင်။အနီးကပ်ဆက်သွယ်မှုစနစ် NFC, Bluetooth ကြိုးမဲ့အနီးကပ်ဆက်သွယ် Wifi Direct မှတဆင့် ဖိုင်ပို့ခြင်းသင့်ရဲ့ဖုန်းမှာ တပါတည်းဖြစ်သော Bluetooth, NFC ကြိုးမဲ့အနီးကပ် ဆက်သွယ်စနစ်၊ Wifi Direct or NFC app နဲ့ feature အဂါရပ်များက အနီးမှာရှိတဲ့စက်တွေကို မျှဝေရာမှာ ရွေးချယ်ဖို့ ခွင့်ပြုပါလိမ့်မယ်ဖုန်းနှစ်ခုလုံးမှာ ဖိုင်တွေက Files By Google Installed နဲ့ သိမ်းထားတာဆိုရင် ဖိုင်တွေကို ဒီနည်းပညာတွေသုံးပြီး app အချင်းချင်း အော့ဖ်လိုင်းနဲ့ မျှဝေနိုင်ပါသည်။Files by Google ကနေ အော့ဖ်လိုင်းနဲ့ ဖိုင်များပို့ခြင်း။

အရေးကြီးမှတ်ချက်။ ဒီဝန်ဆောင်မှုတွေကတော့ ဆက်သွယ်ဖို့လွယ်ကူပြီး အားနည်းချက်ကတော့ လုံခြုံမှုမရှိပါ. Bluetooth and wifi များသည် တည်နေရာဒေသကို ခြေရာခံခြင်း သင့်ဖုန်းdeviceအချက်အလက်တွေကို စုံစမ်းစစ်ဆေးလို့ရနိုင်ပါသည်။ ကြားဖြတ်ဖောက်ထွင်းသူများကလည်း သင့်ဖုန်းdevice ကို စုံတွဲဆက်သွယ်ဖို့ ကြိုးပမ်းတာမျိုးမလိုချင်တဲ့ဖိုင်တွေကိုပို့လိုက်တာမျိုးသို့မဟုတ်ထိခိုက်လွယ်တဲ့အခြေအနေမှာသင့်ဖုန်းdevice ကိုထိန်းချုပ်တာမျိုးတွေလုပ်နိုင်ပါသည်။**ပုံပြီးလုံခြုံမှုရှိဖို့ဆိုရင်စက်တွေကိုမသုံးတဲ့အချိန်မှာ ဝန်ဆောင်မှုတွေအားလုံးကိုပိတ်ထားပြီး လုံခြုံသောနေရာမှ ပြန်ဖွင့်တာမျိုး app တွေကို လိုအပ်တာဘဲ ဘာလဲ/ဘယ်သူလဲခွင့်ပြုချက်ကန့်သတ်ထားတာမျိုးဖုန်းလုံခြုံရေးစနစ်ကိုလေ့ကျင့်ပြီးupdateအမြဲလုပ်နေ**

တာမျိုး ခိုင်မာသောလျှို့ဝှက်နံပါတ် passcode ထားတာမျိုးလုပ်ရမှာဖြစ်သည်။

သီးသန့်ဖော်ပြခြင်း/metadata များပါဝင်စေခြင်း

OTG drive ဆီကို ကြိုးမဲ့drive သို့မဟုတ် ဖုန်းအဟောင်းတွေကနေ မီဒီယာတွေကော်ပီလုပ်တဲ့အခါ ဖော်ပြသောအချက်အလက်များ ပါဝင်စေခြင်း သို့မဟုတ် metadata ကို မီဒီယာနဲ့ သီးသန့်ခွဲထားခြင်းသည် အသုံးဝင်သည်။ မှတ်တမ်းတင်သော app အများစုသည် CSV သို့မဟုတ် JSON မှတ်တမ်းများကို ထုတ်လုပ်ပြီး စက်မှာရှိသော metadata (ဥပမာ ပထဝီအရပ်ဒေသ အချိန် ရက်စွဲ) များကိုရော သုံးစွဲသူက လက်နဲ့ထည့်ထားသောဖော်ပြချက်မှန်သမျှကိုပါဆွဲထုတ်လေ့ရှိသည်။ပြင်ပသို့ထုတ်ပို့ခြင်းလုပ်သည့်အခါ အထက်ပါ metadata များကိုပါ ပါဝင်အောင် မှတ်တမ်းတင်ပြီး အရန်သိမ်းဆည်း backup ထားသင့်သည်။

Drive ကို ကာကွယ်သော လျှို့ဝှက်နံပါတ်

ကြိုးမဲ့drive အများစုသည် မိုဘိုင်းappလျှို့ဝှက်နံပါတ်နဲ့ ကာကွယ်နိုင်သည်။
လျှို့ဝှက်နံပါတ်ဖြင့်ကာကွယ်ခြင်းသည် လျှို့ဝှက်ထိန်းသိမ်းခြင်း encryption နဲ့ မတူသည်ကို သတိပြုပါ။ ကြိုးမဲ့သို့မဟုတ်OTG drive များသည် ကွန်ပျူတာ ဓာတ်ပြားအပြည့် လျှို့ဝှက်ထိန်းသိမ်းခြင်း encryption လုပ်ဆောင်နိုင်သော်လည်း မိုဘိုင်းဖုန်းသုံးရုံဖြင့် မလုပ်ဆောင်နိုင်ပါ။

ဖိုင်များကို လျှို့ဝှက်ထိန်းသိမ်းခြင်း encryption လုပ်ရန် စဉ်းစားပါ

သင့်ရဲ့ဖိုင်များကိုပိုမိုလုံခြုံစိတ်ချစွာစုဆောင်းထားချင်လျှင်အရန်သိမ်းဆည်းခြင်းbackupများကို လျှို့ဝှက်ထိန်းသိမ်းခြင်း encryption လုပ်ရန် စဉ်းစားပါ။ ကြိုးမဲ့စနစ် သို့မဟုတ်OTG drives ပါသော မိုဘိုင်းဖုန်းအများစုကို encryption လျှို့ဝှက်ထိန်းသိမ်း၍ မရနိုင်သော်လည်းဖိုင်များကိုယ်တိုင်ကို အခြား drive ထဲကို မရွှေ့မီတွင် encrypt လျှို့ဝှက်ထိန်းသိမ်းထားနိုင်သည်။ ZArchiver and RAR ကဲ့သို့ app များသည် Android ပေါ်တွင် ဖိုင်များကို encrypt လျှို့ဝှက်ထိန်းသိမ်းထား နိုင်သည်။ ကိုယ့်ရဲ့ encryption လျှို့ဝှက်နံပါတ်ကိုသတိရနေဖို့အတွက်သတိထားပါ။အကယ်၍လျှို့ဝှက်နံပါတ်passwordပျောက်သွားလျှင် ıencryptedလျှို့ဝှက်ထိန်းသိမ်းထားသောဖိုင်များအားပြန်လည်ဖော်ယူရန်နည်းလမ်းမရှိတော့ပါ။
သတိပြုရန်မှာ အချို့နိုင်ငံများမှာ encryption လျှို့ဝှက်ထိန်းသိမ်းခြင်းကို ဥပဒေအရတားမြစ်တာ သို့မဟုတ် ရာဇဝတ်မှုပြုတာမျိုးတွေရှိတတ်ပါသည်။ အာဏာပိုင်တွေကသင့်ရဲ့အချက်အလက်တွေကို ရှာဖွေလို့မရအောင် ကာကွယ်ဖို့သုံးတာဖြစ်ပေမယ့် သက်သေကိုဖျက်ဆီးမှု စုံစမ်းစစ်ဆေးခြင်းကို ပိတ်ဆို့မှု စတဲ့ပြစ်မှုများဟာ ရာဇဝတ်မှုအဖြစ် အပြစ်ပေးခံရနိုင်ပါသည်။ ဒီမြေပုံက (2017 map) ရက်လွန်နေပြီ ဖြစ်သော်လည်း သင့်နိုင်ငံရဲ့ ဥပဒေနဲ့ပတ်သက်ပြီးမေးစရာရှိရင်နေရာတို့ရဲ့အစအနေနဲ့ ပံ့ပိုးမှုဖြစ်ပါသည်။

သီးခြားနေရာများတွင် အရန် ၂ခု ပြုလုပ်သိမ်းဆည်းခြင်း

တခုတည်း အရန်သိမ်းဆည်းတာက ယုံကြည်စိတ်ချစရာမဖြစ်ပါ။ ဥပမာ အရန်သိမ်းထားတဲ့ device ပျောက်တယ် ပျက်တယ် သို့မဟုတ် တခုခု ရှုံးနိမ့်တာမျိုး ဖြစ်နိုင်တယ်။ အိုင်တီကျွမ်းကျင်သူတွေ အကြံပေးတာက သိမ်းတဲ့အခါနှစ်ခု နှစ်နေရာသိမ်းတာဆိုရင် (သုံးစုံဖြစ်သွားပြီ) နောက်စက်တခုထဲထည့်ပြီး

သီးသန့်တနေရာမှာထားရင် ဘယ်တခုပဲ ပျောက်ပျောက် ဖြစ်နိုင်ချေရှိသော အန္တရာယ်များကို ကာကွယ်ပြီးဖြစ်လိမ့်မည်။

အင်တာနက်ဖြတ်တောက်ချိန်တွင် ဖိုင်ဝေမျှခြင်းနှင့် ဆက်သွယ်ခြင်း

ကက်ရှမီးယားဒေသမှာဆက်လက်ဖြစ်ပွားနေဆဲဖြစ်တဲ့ အင်တာနက် ဖြတ်တောက်ခြင်းနှင့် ဖြိုခွဲနှိမ်နင်းခြင်းသည်
ဒီမိုကရေစီစနစ်တွင်းတွင်အကြာရှည်ဆုံးသောအင်တာနက်ဖြတ်တောက်မှုဖြစ်ပြီးဒေသတွင်းရှိ ပြည်သူများ၏အသက်ကို [ပြင်းထန်ထိခိုက်သောသက်ရောက်မှု](#) ဖြစ်စေခဲ့သည်။ ထိခိုက်ဒဏ်ရာပေါ်တွင် ရိုင်းပြစွာစော်ကားခြင်းဆင့်၍ ဒီဇင်ဘာ ၂၀၁၉တွင် WhatsApp၏ ရက် ၁၂၀ သုံးစွဲသူ မူဝါဒအရ ကက်ရှမီးယား၏ [WhatsApp အကောင့်များသည် စတင်၍ ပိတ်သိမ်းခြင်းခံခဲ့ရသည်။](#)

ယခုစာရေးသားသောအချိန်၊ဇန်နဝါရီ(၂၀၂၀)တွင်ကက်ရှမီးယားဒေသ၏အကန့်အသတ်မဲ့ အင်တာနက်ဖြတ်တောက်ခြင်းသည်[တရားမဝင်သောအာဏာအလွဲသုံးစားမှု](#)ဖြစ်သည်ဟုအိန္ဒိယနိုင်ငံ၏ နိုင်ငံတော်တရားရုံးချုပ်တရားဝင်ဆုံးဖြတ်ခဲ့သည်။ ကန့်သတ်ထားသော မြန်နှုန်းမြင့်အင်တာနက် ဘရော့ဘင်နှင့် မိုဘိုင်းအင်တာနက်ကို အချို့နေရာများတွင် ပြန်လည်ရရှိသော်လည်း ခွင့်ပြုသောစာရင်း သန့်ရှင်းသောစာရင်း ဝက်ဘ်ဆိုက်များကိုသာရွေးချယ်ခွင့်ရှိသည်။အင်တာနက်ဖြတ်တောက်ခြင်းများသည်လူအများအားသတင်းအ ချက်အလက်မျှဝေခြင်းနှင့် ဆက်သွယ်ခြင်းအား ပိတ်ဆို့တားဆီးရန် ဒီဇိုင်းလုပ်ထားပြီး (လူများအား မိုဘိုင်းဖုန်းနှင့် SMS အချက်ပို့ခြင်း စသဖြင့် လုံခြုံမှုနည်းသော ဆက်သွယ်ရေးပုံစံစနစ်များကိုသာ သုံးရန် တွန်းပို့ခြင်းဖြင့်အာဏာပိုင်များအနေဖြင့်ကြားဖြတ်နားထောင်ခြင်းလေ့လာစောင့်ကြည့်ခြင်းများကို လွယ်ကူစေသည်) ။ကက်ရှမီးယားဒေသ၏ အတင်းကြပ်ဆုံးအင်တာနက်ဖြတ်တောက်ချိန်များ အတွင်းတွင် လူများစုသည် [လက်ရေးစာများသုံးခြင်း စာပို့စာယူစနစ်များ](#) သုံးခြင်းကိုသာ ယင်းတို့၏ချစ်ခင်သူများနှင့် သတင်းစကားပါးရန်အခြားရွေးချယ်စရာမရှိ၍ရွေးချယ်စရာအဖြစ်သတ်မှတ်ခဲ့ရသည်။ပိတ်ဆို့တားဆီးခြင်းအ ားလုံးကိုရှောင်တိမ်းနိုင်ရန် သေချာပေါက်နည်းလမ်း မရှိသေးသော်လည်း တက်ကြွလှုပ်ရှားသူနှင့် မိတ်ဆွေတို့၏ စကားလက်ဆုံများမှတဆင့် ကျွန်ုပ်တို့လေ့လာခဲ့သည်မှာ အချို့သော နည်းလမ်းများနှင့် ချဉ်းကပ်နည်းများသည် အော့ဖ်လိုင်းမျှဝေခြင်းနှင့် ဆက်သွယ်ခြင်းများ အခြေအနေပေါ်မူတည်ပြီး သင့်အတွက် အလုပ်ဖြစ်နိုင်မည်။
မှတ်ချက်ပြုရန်မှာ အချို့ရွေးချယ်နိုင်သောလမ်းများသည် စတင်ပြင်ဆင် setup လုပ်ရန်အတွက် အင်တာနက်လိုအပ်သည်။ (app ဒေါင်းလုပ်လုပ်ခြင်း စသဖြင့်)

အနီးကပ်ဆက်သွယ်မှုစနစ် NFC, Bluetooth ကြိုးမဲ့အနီးကပ်ဆက်သွယ် Wifi Direct မှတဆင့် ဖိုင်မျှဝေခြင်း

သင်ဖုန်းနဲ့ နီးရာတွင်ရှိသော ဖုန်းသို့မဟုတ်device တခုကိုဆက်သွယ်ရန် အင်တာနက်ဆက်သွယ်မှုရှိရန် မလိုအပ်ပါ။Bluetooth,Wifi,Direct,NearFieldCommunicationNFC/နီးစပ်ရာကွင်းပြင်ဆက်သွယ်စနစ် အင်တာနက်မလိုအပ်ပါ။(တခါတရံ အင်ဒရိုက်ဘိန်းဟုလည်းခေါ်သည်)။Bluetooth နှင့် Wifi Direct နှစ်ခုစလုံးသည် ကြိုးမဲ့ဆက်သွယ်နည်းပညာ ဖြစ်ပြီ ဖုန်းသို့မဟုတ်deviceနှစ်ခုကို ချိတ်ဆက်ပို့ဖိုင့် သို့မဟုတ် ကွန်ယက်ဖြန့်ချီစက် မရှိဘဲ “စုံတွဲဆက်သွယ်” နိုင်ပါသည်။ Wifi Directက ပိုမိုကျယ်ဝန်းသော အကွာအဝေးကို

Bluetooth
ထက်ပို၍လျင်မြန်သောဒေတာလွှဲပြောင်းမှုပံ့ပိုးနိုင်ပါသည်၊သို့သော်ပါဝါကိုအလွန်တရာပိုသုံးသည်။
တချိန်တည်းမှာ NFC သည် ပိုမိုတိုတောင်းသော အကွာအဝေးကို Bluetooth or Wifi Direct ထက်နှေးသော လွှဲပြောင်းနှုန်းဖြင့် သို့သော် ပိုမိုမြန်ဆန်စွာချိတ်ဆက်ပြီး ပါဝါသုံးနှုန်းနည်းသည်။ ထို့ကြောင့် ပမဏာနည်း လွှဲပြောင်းခြင်းဖြစ်မယ် စက်နှစ်ခုလုံးလက်ထဲရှိမယ်ဆို အသုံးဝင်သည်။
Wifi Directကတော့ဘလူးတုထက်စာရင်ဝေးဝေးရောက်ပြီး ဒေတာတွေကို မြန်မြန်ပြောင်းရွှေ့နိုင်စွမ်းရှိပေမယ့် ပါဝါသုံးတာအရမ်းများပါသည်တချိန်တည်းမှာNFCအနီးကပ်ဆက်သွယ်မှုလေးစင်တီမီတာပိုပြီးနီးနီးအကွာအဝေးနဲ့ ပြောင်းရွှေ့ချိန်လည်းပိုနှေးကွေးပါသည်သို့သော် သူက ဆက်သွယ်မှုပိုမြန်ပြီး ပါဝါသုံးတာပိုနည်းတာမို့ ခပ်မြန်မြန်နဲ့ နည်းနည်းပဲ ပြောင်းရွှေ့မယ် စက်နှစ်ခုလုံးလက်ထဲမှာရှိမယ်ဆို အသုံးဝင်ပါတယ်။
သင့်ရဲ့ဖုန်းမှာBluetooth, Wifi Direct or NFC features အင်္ဂါရုပ်များက တပါတည်းပါလာပြီး မျှဝေဖို့နည်းလမ်းများကိုလည်း ပြသထားနိုင်ချေရှိပါသည်။ ဒါ့အပြင် ဖိုင်းတွေကိုမျှဝေတဲ့ အင်္ဂါရုပ်မျိုးဖြစ်တဲ့ Files by Google app ကဲ့သို့နည်းပညာများလည်း ပေါင်းစပ်ထားမှာပါ။

အရေးကြီးမှတ်ချက်။ဒီဝန်ဆောင်မှုတွေကတော့ ဆက်သွယ်ဖို့လွယ်ကူပြီး အားနည်းချက်ကတော့ လုံခြုံမှုမရှိပါ။ Bluetooth and wifi များသည် တည်နေရာဒေသကို ခြေရာခံခြင်း သင့်ဖုန်းdeviceအချက်အလက်တွေကို စုံစမ်းစစ်ဆေးလို့ရနိုင်ပါသည်။ ကြားဖြတ်ဖောက်ထွင်းသူများကလည်း သင့်ဖုန်းdevice ကို စုံတွဲဆက်သွယ်ဖို့ ကြိုးပမ်းတာမျိုး မလိုချင်တဲ့ဖိုင်တွေကို ပို့လိုက်တာမျိုး သို့မဟုတ် ထိခိုက်လွယ်တဲ့အခြေအနေမှာ သင့်ဖုန်းdeviceကို ထိန်းချုပ်တာမျိုးတွေ လုပ်နိုင်ပါသည်။**ပိုပြီးလုံခြုံမှုရှိဖို့ဆိုရင် စက်တွေကို မသုံးတဲ့အချိန်မှာ ဝန်ဆောင်မှုတွေအားလုံးကိုပိတ်ထားပြီး လုံခြုံသောနေရာမှ ပြန်ဖွင့်တာမျိုး app တွေကို လိုအပ်တာဘဲ ဘာလဲ/ဘယ်သူလဲခွင့်ပြုချက် ကန့်သတ်ထားတာမျိုး ဖုန်းလုံခြုံရေးစနစ် ကိုလေ့ကျင့်ပြီး update အမြဲလုပ်နေတာမျိုး ခိုင်မာသောလျှို့ဝှက်နံပါတ် passcode ထားတာမျိုးလုပ်ရမှာဖြစ်သည်။**

ကြိုးမဲ့စနစ်ဖြင့်ဖိုင်များကိုမျှဝေခြင်း ကြိုးမဲ့ဆက်သွယ်မှုဧရိယာကွန်ယက်

ကြိုးမဲ့hard drive သို့မဟုတ် flash drive များကို အဖွဲ့တွင်း သို့မဟုတ် လူများစုကို တပြိုင်နက်တည်း ဖိုင်မျှဝေရာတွင် သုံးနိုင်သည်။Wifi driveသည်များသောအားဖြင့် ညွှန်ကြားချက်များနှင့်အတူ သို့မဟုတ် drive ဆက်သွယ်ရန် app များပါပြီး သုံးစွဲရန် လွယ်ကူသည်။ လုံခြုံရေးအတွက် drive ကို လျှို့ဝှက်နံပါတ်လုပ်ရန် သတိရပါစေ။ကြိုးမဲ့driveမရှိဘူးဆိုရင်ပုံမှန်USBdriveကိုကြိုးမဲ့ကွန်ယက်ဖြန့်ချီကိရိယာမှာပလပ်ထိုးပြီးသုံးလို့ရပါသည်။USBအပေါက်ပါသောခရီးသွားကွန်ယက်ဖြန့်ချီကိရိယာသည်စျေးသက်သာပြီးသယ်ယူရန်လွယ်ကူသည်။သုံးစွဲသူသည်USBdriveကိုအင်တာနက်မလိုဘဲဒေသတွင်းဧရိယာကွန်ယက်မှတဆင့်ဆက်သွယ်နိုင်သည်
။
ဖုန်းထဲမှာရှိသောဖိုင်များကို USB drive နှင့် ဝင်ရောက်ချိတ်ဆက်ရန် ဖိုင်မန်နေဂျာ app ကို သုံးစွဲပြီးSolid Explorer ကဲ့သို့ကွန်ယက်တွင်းရှိ သိုလှောင်ခန်းများကို ဆက်သွယ်နိုင်သည်။ ကွန်ယက်ဖြန့်ချီကိရိယာ၏ အိုင်ပီလိပ်စာကို သင့်ဖုန်း၏ advanced wifi settings တွင် တွေ့ရှိနိုင်သည်။
နောက်တခုသုံးနိုင်တဲ့ နည်းလမ်းတခုက PirateBox လို့ခေါ်တဲ့ ကိုယ်တိုင်လုပ် ပရောဂျက်ဖြစ်ပြီးတော့ လိုင်စင်ရှိဖရီးဆော့ဖ်ဝဲဖြစ်သည်။အပေါ်မှာပြထားသလိုပဲဖိုင်တွေကိုမျှဝေနိုင်ပြီးPirateBoxကအမည်မသိမျှဝေ

ခွင့်ပေးမှာဖြစ်တဲ့အပြင်ချက်နဲ့ မတ်ဆေ့ပို့နိုင်တဲ့ အဂါရပ်များလည်းပါဝင်ပါသည်။ PirateBox ကိုပြင်ဆင်ခြင်း setupလုပ်ဖို့အတွက် ဆော့ဖ်ဝဲ အပိုင်းအစအနည်းငယ်ကို download, install နဲ့ setup လုပ်ရမှာဖြစ်ပါသည်။ ညွှန်ကြားချက်များကို Pirate Box ဝက်ဘ်ဆိုက်တွင် ကြည့်ပါ။

မိတ်ဆွေချင်းချက်လုပ်ပြီးဆက်သွယ်ခြင်း

တက်ကြွလှုပ်ရှားသူကွန်ယက်များမှတစ်ဆင့်သတိပြုမိလာတဲ့အသစ်ကဲ့သို့ မိတ်ဆွေချင်းအချက်ပို့ဆက်သွယ်တဲ့ app များတွင် Briar and Bridgefy တို့ဖြစ်သည်။ကျွန်ုပ်တို့ သုံးစွဲဖူးခြင်းမရှိသေးသော်လည်း စမ်းသပ်သုံးစွဲဖူးသူများကို သိရှိပါသည်။

Briar သည် ပွင့်လင်းအရင်းအမြစ်ဖြစ်ပြီး နှစ်ဖက်လုံးလျှို့ဝှက်ထိန်းသိမ်း သောစနစ်ဖြင့် အချက်ပို့သောapp ဖြစ်ပြီးဗဟိုဆာဗာကို အားကိုးခြင်းမရှိဘဲသုံးစွဲသူများ၏ဖုန်း(device)များကိုsyncsဆွဲယူခြင်း(သုံးစွဲသူတိုင်း၏ device တွင် အကြောင်းအရာများကို အသက်ဝင်နေမည်။အင်တာနက်မသုံးဘဲ Bluetooth or Wifi သုံးရုံဖြင့်လည်း ဆွဲယူနိုင်သည်။ (အင်တာနက်ရချိန်တွင် Tor ကွန်ယက်ကိုသုံးပြီး ဆွဲယူနိုင်သည်) Briar သည် ကိုယ်ပိုင်အုပ်စုဖွဲ့ခြင်း အများသုံးဖိုရပ်များ ဘလော့ဂ်များလည်း တည်ဆောက်နိုင်သော အဂါရပ်များပါသည်။ အော့ဖ်လိုင်းသုံးချိန်တွင် သင်၏အကွာအဝေးသည် Bluetooth or Wifi အကွာအဝေးကဲ့သို့ ကန့်သတ်ချက်ရှိသည်။ (အများဆုံး တရာမီတာ)
တချိန်တည်းတွင်Bridgefyသည်နှစ်ဖက်လုံးလျှို့ဝှက်လုံခြုံသော(တိုက်ရိုက်အသံလွှင့်သောအဂါရပ်သုံးခြင်းမှ အပ) အချက်ပို့သော app ဖြစ်ပြီး Bluetooth ကိုသုံးပြီး အချက်ပို့သည်။ Brairနဲ့မတူသောအချက်က မတ်ဆေ့သည်အကွာအဝေးရှည်ရှည်ခရီးရောက်နိုင်သည်။အခြားBridefyသုံးစွဲသူများ၏ပိုက်စိတ်တိုက်ထား သောကွန်ယက်မှ ခုန်ဆွခြင်း (ရည်ရွယ်ပြီးပို့သူသာဖတ်လို့ရမည်ဖြစ်သည်)။ Bridgefy သည် Briar ကဲ့သို့ ကိုယ်ပိုင်အဖွဲ့ဖိုရမ်၊ဘလော့ဂ်အဂါရပ်များမပါရှိသော်လည်းတိုက်ရိုက်လွှင့်သောစွမ်းရည်ရှိပြီးတပြိုင်တည်းတွင် သင့်ဆက်သွယ်သူ စာရင်းထဲတွင် မပါသော Bridgefy သုံးစွဲသူ ၇ ယောက်ဆီအထိ ပို့နိုင်သည်။ (လိုအပ်ချက်အရ တိုက်ရိုက်လွှင့်သော မတ်ဆေ့များသည် လျှို့ဝှက်ထိန်းသိမ်းခြင်း encrypted မဖြစ်ပါ)။

လျှို့ဝှက်ထိန်းသိမ်းSMSမှတဆင့်ဆက်သွယ်ခြင်း

ဖုန်းလိုင်းနဲ့သွားသော အချက်ပို့ခြင်းသည် အက်စ်အမ်အစ်ပို့ခြင်းသည် အင်တာနက်အပေါ်မှီကပ်စရာမလိုပါ၊ အင်တာနက်ဖြတ်တောက်ထားခြင်းတွင်လည်း အသုံးပြုနိုင်သည်။ သို့သော် လုံခြုံမှုလုံဝမရှိပါ။ အင်တာနက်ရှိမှ သုံးလို့ရသော app များဖြစ်သည့် WhatsApp or Signal နဲ့မတူသည်မှာ SMS သည် နှစ်ဖက်စလုံးကို လျှို့ဝှက်ထိန်းသိမ်းထားခြင်းမရှိဆိုလိုသည်မှာ အချက်ပို့ခြင်းနှင့် သူတို့၏ metadataများသည် အစိုးရနည်းတူ ဖုန်းဝန်ဆောင်မှုပေးသူများဟတ်ကာများကကြားဖြတ်၍ထိုအချက်ပို့ခြင်းများကိုဖတ်ရှုနိုင်သည်။ SMSများသည်လှည့်စားနိုင်သည်။ဆိုလိုသည်မှာပို့ပေးသူသည်သူတို့၏လိပ်စာအချက်အလက်ကိုလိမ်လည်ပြီး တခြားသူအနေနဲ့ အယောင်ဆောင်ပြီးပေးပို့နိုင်သည်။
SMS ပို့စရာရှိလျှင် Silence ဆိုတဲ့ app သည် နှစ်ဖက်စလုံးကို လျှို့ဝှက်ထိန်းသိမ်းထားသော SMS ဖြစ်သည်။ ပွင့်လင်းအရင်းအမြစ်ဖြစ်ပြီးSignal၏လျှို့ဝှက်ထိန်းသိမ်းခြင်းလုပ်ထုံးလုပ်နည်းကိုသုံးထားသည်။ကျွန်ုပ်တို့ကို ယ်တိုင်စမ်းသပ်ဖူးခြင်းမရှိသော်လည်းအခြားသူများသုံးသည်ကိုကြားဖူးသည်။ပေးပို့သူရောလက်ခံသူပါinstall

လုပ်ထားရမှာဖြစ်ပြီးလဲလှယ်သောသော့ချက်ရှိရမှာဖြစ်သည်။SMSသည်သင့်ရဲ့တယ်လီကွန်းဆာဗာကိုဖြတ်ပြီး မှသွားမှာဖြစ်တဲ့အတွက်Silenceကိုသုံးရင်တောင်မှလျှို့ဝှက်သောမတ်ဆေ့ကိုပို့မှာဖြစ်သော်လည်း မတ်ဆေ့ရဲ့metadata တွေကိုတော့ တယ်လီကွန်း ကုမ္ပဏီတွေကနေ အချက်အလက်ရှာဖွေနိုင်မှာ ဖြစ်ပါသည်။

တစ်စိတ်တစ်ပိုင်းဖြတ်တောက်ခြင်းပိတ်ပင်တားဆီးထားသောဆိုက်ဒ်များကိုရှောင်တိမ်းခြင်း

မကြာခဏအားဖြင့် အင်တာနက်ဖြတ်တောက်ခြင်းသည် အင်တာနက်တစ်ခုလုံး ပြတ်အောင်ပိတ်ခြင်းမဟုတ်ဘဲ အချို့သီးခြားဝက်ဘ်ဆိုက်ဒ်နှင့်ဆိုရှယ်မီဒီယာများကိုသာပိတ်ပင်ခြင်းလည်းဖြစ်နိုင်သည်။အာဏာပိုင်အစိုးရသည်အင်တာနက်ဝန်ဆောင်မှုပေးသူISPများမှတစ်ဆင့်အိုင်ပီလိပ်စာပေါ်အခြေခံသောပိတ်ပင်ခြင်း အကြောင်းအရာသို့မဟုတ် DNS looups ဒိုမိန်းအမည်စနစ်ရှာဖွေခြင်းစနစ်ကတစ်ဆင့် ပိတ်ပင်နိုင်သည်။ ဆိုက်ဒ်တခုကပိတ်ပင်ထားခြင်းခံရသလားဆိုတာမသေချာဘူးလားအဖွဲ့အစည်းများဖြစ်သော Open Observatory of Network Interference and Netblocks စသောအဖွဲ့အစည်းများက လေ့လာစောင့်ကြည့်ချင်း အင်တာနက်ပြတ်တောက်မှုနဲ့ ပတ်သက်ပြီး တိုင်းတာခြင်း ဆင်ဆာဖြတ်ခြင်းကို ကမ္ဘာနှင့်တဝန်းတွင်လုပ်ဆောင်သည်။ကံကောင်းထောက်မသည်မှာသင့်တွင်အင်တာနက်ဝင်ရောက်ချိတ်ဆက်ခွင့် ရှိသမျှ ကာလပတ်လုံး တစ်စိတ်တစ်ပိုင်းပိတ်ဆို့ခြင်းကို ကျော်ဖြတ်နိုင်သော နည်းလမ်းများရှိသေးသည်။ လျှို့ဝှက်ထိန်းသိမ်းခြင်းencryptionနှင့်အတူပိတ်ဆို့ထားသောဆိုက်ဒ်များကိုရှောင်တိမ်းပြီးအသုံးပြုခြင်းသည်လည်း သင့်နိုင်ငံတွင် ရာဇဝတ်ပြစ်မှုအဖြစ်သတ်မှတ်နိုင်ကြောင်း သတိပြုပါ။

ဗီပီအန် ခေါ်လျှို့ဝှက်ဆက်သွယ်ကွန်ယက်

အိုင်ပီအခြေခံနှင့်အကြောင်းအရာကိုအခြေခံသောပိတ်ပင်တားဆီးခြင်းကိုရှောင်ကွင်းကျော်ဖြတ်ရန်နည်းလမ်းတခုမှာProtonVPNorTunnelBearကဲ့သို့လျှို့ဝှက်ကွန်ယက်စနစ်ဗီပီအန်သုံးခြင်းဖြစ်သည်။ ဗီပီအန်မှတစ်ဆင့်ဆက်သွယ်သောအခါအင်တာနက်အသွားအလာလမ်းကြောင်းသည်လျှို့ဝှက်လုံခြုံပြီးဗီပီအန်ဆာဗာမှတစ်ဆင့်တစ်ခြားအရပ်ဒေသ၊အခြားနိုင်ငံအစရှိသဖြင့်ပြောင်းသွားပြီးအမှန်တကယ်ရည်ရွယ်ရာအရပ်နှင့်သင့်အင်တာနက်အသွားအလာလမ်းကြောင်းအကြောင်းအရာကိုသင့်အင်တာနက်ဝန်ဆောင်မှုပေးသူအားဖုံးကွယ်သည်။
ဖြတ်သန်းသွားသောကြောင့်တကယ်နေရာအစစ်အမှန်နဲ့ပါဝင်မှုများကိုလမ်းကြောင်းပြောင်းပေးသည်။ တချို့နိုင်ငံအစိုးရများက ဗီပီအန်သုံးစွဲမှုကို ပိတ်ပင်ခြင်း သို့မဟုတ် ပိတ်ထားသော ဗီပီအန်မှ တဆင့်သုံးစွဲမှုကို ခြေရာခံခြင်းများ လုပ်နိုင်သည်။ အရေးကြီးသည်မှာစိတ်ချရသော ဗီပီအန်ကိုသုံးစွဲခြင်း အချက်အလက်များကို မစုဆောင်းသောတစ်ခုကိုသုံးစွဲခြင်းကိုပြုသင့်သည်။မည်သည့်နိုင်ငံတွင်ဗီပီအန်ကရှိနေသလဲသူတို့ရဲ့ ဆုံးဖြတ်သုံးသပ်မှုများသည်တရားဆိုင်ရာလမ်းကြောင်များရှိမရှိတစ်ချို့အစိုးရသည်ဗီပီအန်ကိုခွင့်ပြုသော်လည်းသင့်အချက်အလက်များကို စုံစမ်းထောက်လှမ်းခြင်း လေ့လာစစ်ဆေးခြင်းများလုပ်ဆောင်သည်။

DNS ဆာဗာ ဒိုမိန်းအမည်စနစ်

DNS (ဒိုမိန်းအမည်စနစ်) ဆာဗာတွေဟာ ဒိုမိန်းအမည်တွေကို ဘာသာပြန်ပြီး အလုပ်လုပ်တဲ့ သို့မဟုတ် သုံးစွဲသူအနေနဲ့ နံပါတ်ပါသော အိုင်ပီလိပ်စာများကို ရိုက်ထည့်ပြီး အင်တာနက် ဝက်ဘ်စာမျက်နှာတွေကို ခွဲခြားသတ်မှတ်တဲ့ URL တွေ ဖြစ်ပါသည်။ ISP အင်တာနက်ဝန်ဆောင်မှုပေးသူသည် ဒိုမိန်းအမည်စနစ် DNS

ဆာဗာများကို ပြုပြင်ပြီး အချို့မေးမြန်းချက်များကို ထိန်းချုပ်ခြင်း ဝက်ဘ်ဆိုက်ဒ်မရှိပါ ဟူ၍ မမှန်သောစာမျက်နှာများကိုပြန်ပို့ခြင်းလုပ်သည်။
၂၀၁၄ ခုနှစ် တူရီကီရွေးကောက်ပွဲကာလအတွင်း တူရကီဝန်ကြီးချုပ် Recep Tayyip Erdogan က တွစ်တာကို ပိတ်ရန်ကြိုးစားတုန်းက ထိုနည်းကိုသုံးခဲ့သော်လည်း ပိတ်ပင်ခြင်းကို တက်ကြွလှုပ်ရှားသူများက လျင်မြန်စွာဖောက်ထွင်းပြီးဗီပီအင်သုံးရန်နှင့်ဒိုမိန်းအမည်စနစ်DNSဆာဗာပြောင်းရန်အသုံးဝင်သည့်အချက်များကို တဆင့်ပြီးတဆင့် တဆင့်ချင်း တားဆီးနိုင်နိုင်ခဲ့သည်။

မူလDNSဆာဗာကို ဖုန်းရဲ့network သို့မဟုတ် wifi setting မှာ ပြောင်းလို့ရပါသည်။ ဆာဗာသုံးတဲ့အခါ မူလDNSဆာဗာ တမျိုးတည်းမသုံးဘဲ အပြောင်းအလဲဆာဗာတွေဖြစ်တဲ့ Google Public DNS or quad9 တွေကို ပြောင်းလဲသုံးခြင်းဖြင့် DNSကို အခြေခံပြီး ပိတ်ဆို့တာတွေကို လှည့်ပတ်သွားနိုင်မှာဖြစ်ပါသည်။ Quad 9 တွင်Quad 9 Connect . ဟုခေါ်သော app တစ်ခုလည်းရှိသည်။ယခုစာရေးနေသည့်အချိန်တွင် Quad9 connect appသည် စတင်အသုံးပြုနိုင်ရန် စမ်းသပ်သည့်အဆင့်မှာသာရှိသေးသည်။

ပိတ်ပင်ခြင်းကိုရှောင်တိမ်းနိုင်သောအသုံးများသည့်နည်းလမ်းနှစ်မျိုးသာရှိသည်။
အတွင်းကျကျအချက်အလက်များကိုလေ့လာလိုလျှင်“InternetSociety, AccessNow, Security-in-a-Box and EFF” တွင် အတွင်းကျကျ အချက်အလက်များကိုရရှိနိုင်ပါသည်။