Risk Mitigation and Management Guide

CODE GREEN

ဤလမ်းညွှန် သည် စိုးရိမ်ဖွယ် ရေချိန်အရ ပြင်ဆင်ထားသင့်သော၊ ပုံမှန်ကျင့်သုံးသင့် သောဒစ်ဂျစ်တယ် လုံခြုံရေး အမူအကျင့်များနှင့် ပြင်ဆင်ထားသင့်သည်များကို ပြုစုထားသော လမ်းညွှန်တစ်ခုဖြစ်သည်။ CODE GREEN (အစိမ်းရောင်အဆင့်) ဟု သတ်မှတ်သည့် အခြေအနေများ တွင် မိမိ၏ ဒစ်ဂျစ်တယ် လုံခြုံရေးအား “ ကြိုတင်ကာကွယ်” ထားနိုင်ဖို့ ရည်ရွယ်သည်။

Code Green ဆိုသည်မှာ

- **အင်တာနက်ရရှိနေချိန်**
- **မိမိအား စောင့်ကြည့်မှု၊ ဖမ်းဆီးမှုများရှိမနေသေးသည့်အချိန်**
- **မိမိ၏ ဒစ်ဂျစ်တယ် ပစ္စည်းများကို လုံခြုံရေးတိုးမြှင့်ဖို့ရန်အတွက် အချိန်ကောင်းစွာရရှိနေသေးသည့်အခြေအနေ**

တို့တွင် ဆက်သွယ်လုပ်ဆောင်မှုများ လုံခြုံ စေရန် သတိပြုလိုက်နာသင့်သော အကြံပြုချက်များဖြစ်သည်။

မိမိ ကိုယ်ကိုသော်လည်းကောင်း မိမိအဖွဲ့အစည်းကိုသော်လည်းကောင်း ပစ်မှတ်ထားသည်ဟု ယူဆရသည့် စိုးရိမ်ရေချိန် ပိုမိုတိုးတက်လာပါက CODE YELLOW နှင့် CODE RED လမ်းညွှန်များအား ထပ်မံဖတ်ရှုသင့်သည်။

Application တစ်ခုခုသုံးလိုက်ရုံမျှနှင့် ၁၀၀ ရာခိုင်နှုန်း လုံခြုံဖို့ဆိုသည်မှာ မဖြစ်နိုင်သည်ကို အရင်ဆုံး သတိပြုသင့်သည်။ နေ့စဉ် မိမိ၏ ဒစ်ဂျစ်တယ်လုံခြုံရေးနှင့် ပတ်သက်၍ ဂရုပြုကျင့်ကြံနေထိုင်ခြင်းကသာ ဒစ်ဂျစ်တယ်အရ တိုက်ခိုက်ခံရနိုင်ခြေကို လျှော့ချပေးနိုင်သည့် အကောင်းဆုံး နည်းလမ်းတစ်ခုဖြစ်သည်။

Passwords and Password Managers

- အရေးအခြေအနေများတွင် မိမိ၏ ဖုန်းများ၊ ကွန်ပျူတာများ၏ လျို့ဝှက်နံပါတ်များကို လုံခြုံပြီး ခန့်မှန်းရန် ခက်ခဲသော လျို့ဝှက်နံပါတ်များပေးသင့်သည်။ (လျို့ဝှက်နံပါတ်များပေးရာတွင် မွေးနေ့လိုမျိုး၊ မှတ်ပုံတင်လိုမျိုး ကိုယ်ရေးကိုယ်တာ အချက်အလက်များ မပေးသင့်ပါ။ ခက်ခဲသော လျို့ဝှက်နံပါတ်များပေးသင့်ပါသည်။ (@#!2”N: အစရှိသော မှန်းဆရန် ခက်ခဲသော Password များပေးသင့်ပါသည်။)
- မိမိဖုန်းတွင် အလိုအလျောက်ဖွင့်လို့သော စနစ်များ (လက်ဗွေရာ များနှင့် ဖွင့်သောစနစ်..မျက်နှာပြပြီး ဖွင့်သောစနစ်များထက် လျို့ဝှက်နံပါတ်များသာ ပေးသင့်ပါသည်။
- မိမိဖုန်းထဲတွင်ထည့်ထားသော Mobile Banking Apps များတွင်လည်း လျို့ဝှက်နံပါတ်များကို Face Unlock (မျက်နှာနဲ့ Lock ဖွင့်ခြင်း) ၊ Finger Print (လက်ဗွေရာဖြင့်ဖွင့်ခြင်း) များအစား ကိုယ်တစ်ယောက်သာသိနိုင်မည့် Pin / Passphrase (Alphabet , Number များဖြင့် ထားခြင်း) တို့ကိုသာလုပ်ဆောင်သင့်ပါသည်။
- မိမိတို့၏ email ၊ social media နှင့် အခြားအကောင့်များ၏ password များကို မမှတ်မိပါက reset ချ၍ password အသစ်ပြောင်းလဲပါ။
- Password များအား မိမိ ကိုယ်တိုင် မှတ်ထားခြင်းထက် password manager များအသုံးပြုသင့်သည်။ ထိုကဲ့သို့ အသုံးပြုခြင်းဖြစ် အကောင့်တစ်ခုချင်းစီအတွက် မတူညီသော လုံခြုံသော password များထားရှိနိုင်ပြီး လုံခြုံရေးကို ပိုမိုအားကောင်းစေသည်။
- Password manager တစ်ခုဖြစ်သည့် KeePassXC (for Computers), KeePassDX (for Android), KeePassium (for iPhone) အား လေ့လာ အသုံးပြုရန် တွဲဖက်ပါ guide တွင် ဖတ်ရှုနိုင်ပါသည်။
- Keepass file (.kdbx extension) သည်အလွယ်တကူ upload (သို့) ရွှေ့ပြောင်းမှုပြုလုပ်နိုင်သည်။

- Saved logins ဟုခေါ်သော မိမိ၏ အင်တာနက် browser (Firefox, Chrome, Internet Explorer, etc.) တို့တွင် password များသိမ်းဆည်းထားမှုကိုလည်း ဂရုပြု ရှောင်ရှားသင့်ပါ။

အကောင့်လုံခြုံရေးအား ဂရုထားခြင်း

- မိမိနှင့်မသက်ဆိုင်သည် လင့်ခ်များမနှိပ်ခြင်း
- စကားဝှက်ကို သူများနှင့်မဝေမျှခြင်း
- ဖုန်းနှင့်ကွန်ပျူတာအား စကားဝှက်ခံထားခြင်း
- ဖုန်းအားသူများလွယ်ကူစွာရယူနိုင်သည့် နေရာတွင်မထားခြင်း
- မိမိအကောင့်များအား တစ်စုံတစ်ယောက် ဝင်ရောက်နေသည်ဟု သိရှိပါက မိမိအကောင့်များအား Password အရင်ပြောင်းပြီး ဝင်ရောက်ထားခဲ့သည့် Device တွေထဲကနေ Log out ထွက်ပါ။
- Device တွေ အကုန်လုံးကနေ အလျင်အမြန် Log out ထွက်ခြင်း) (Facebook- Seurity Setting ဝင်ပါ၊ ပြီးရင် Security and Log in ထဲက အပေါ်ဆုံးအပိုင်းလေးမှာ Where you're log in လေးကိုတွေ့ရင်၊ သူ့ဘေးနားက See all လေးကိုနှိပ်လိုက်ပါ။ ပြီးရင် Log out for all sessions ကိုနှိပ်လိုက်ရင် တစ်ခါတည်း Log out ထွက်ပြီးသားဖြစ်မှာပါ။
- Viber တို့ Messenger တို့ကနေ ထိရှလွယ်တဲ့ သတင်းစကားတွေကိုအဖွဲ့ဝင် အချင်းချင်း ဝေမျှပေးလိုလျှင် လုံခြုံအောင် (Secret Conversation လုပ်လို့ရပါသည်)။ Messenger ထဲကိုဝင်ပါ၊ ကိုယ်ပြောမယ့် မိတ်ဆွေဆီကို ဝင်ပါ။ ပြီးလျှင် သူ့ Profile လေးကိုနှိပ်လိုက်မယ်ဆိုရင် Go to Scret Conversation လေးကို နှိပ်လိုက်တာနဲ့ ရသွားပါပြီ။ Message ပို့တဲ့နေရာလေးက အဝိုင်းလေးကတော့ အချိန်သတ်မှတ်တာဖြစ်ပြီး ကိုယ်သတ်မှတ်ထားတဲ့ အချိန်ကျော်တာနဲ့ Message တွေက အလိုအလျောက် ပျက်သွားမှာပါ။
- 99% သော အချက်အလက် ပေါက်ကြားမှုသည် မိမိ၏ Facebook Account (သို့)Gmail ကို နှစ်ဆင့်ခံလုံခြုံရေး 2 Factor Authentication မထားခြင်းကြောင့်ဖြစ်သည်။
- 2 Factor Authentication ထားလိုလျှင် Setting ကနေ Security and Log in ကိုဝင်ပါ။ Use Two Factor authentication တွေ့ပါလိမ့်မယ်။ အဲ့ထဲမှာမှ Text Message ကိုရွေးပြီး မိမိဖုန်းနံပါတ်လေး ထည့်ပေးလိုက်မယ်ဆိုရင် တော်တော်လေးလုံခြုံသွားပြီလို့ ပြောနိုင်ပါပြီ။

အင်တာနက်မှ လုံခြုံစွာဆက်သွယ်ခြင်း

- End to End encryption ထောက်ပံ့ပေးသည့် Instant messenger များကိုအသုံးပြုပါ
- ဖုန်းအသွားအလာများအား ကြားဖြတ်နားထောင်ခြင်းဖြင့်သော်လည်းကောင်း၊ စာတိုပို့လွှတ်မှုအား စောင့်ကြည့်ခြင်းဖြင့်သော်လည်းကောင်း ရယူသွားနိုင်သည်။
- အင်တာနက်မှာ လုံခြုံစွာ ဆက်သွယ်နိုင်ရန် Signal Messenger application ကို ဖုန်းနံပါတ်ဖြင့် မှတ်ပုံတင်ကာ အသုံးပြုနိုင်သည်။ ။
- ဤလင့် တွင် ဝင်ရောက်၍ မည်ကဲ့သို့ စတင်အသုံးပြုကာ ချိတ်ဆက်နိုင်ကြောင်း လေ့လာနိုင်သည်။
- MacOs နှင့် WindowsOS များတွင်ပါ install ပြုလုပ်၍ ချိတ်ဆက် အသုံးပြုနိုင်သည်။
- တွဲဖက် ပါဝင်သော သက်ဆိုင်ရာလမ်းညွှန်များကို ဖတ်ရှု၍ အဆင့်ဆင့်ကို လေ့လာနိုင်ပါသည်။
- အခြေနေတစ်မျိုးမျိုးကြောင့် Signal application အား ပိတ်ဆို့မှုတစ်မျိုးမျိုးပြုလုပ်ထားပါက Signal အလားတူ Wire application သွင်းယူပါ

သတိပြုရန်မှာ အထက်ပါ e2e ဆက်သွယ်မှု ထောက်ပံပေးနိုင်သော application နှစ်ခုလုံးသည် Viber VOIP အလားတူ ပင် ဆက်သွယ်မှုပြုလုပ်ရန်အတွက် နှစ်ဦးလုံး သို့ ဆက်သွယ်မှုပြုလုပ်လိုသည့် သူများအချင်းချင်း application ရှိမှသာဆက်သွယ်မှုပြုလုပ်နိုင်မည်ဖြစ်သည်။

ဖုန်းလိုင်းမှ လုံခြုံစွာဆက်သွယ်ခြင်း

- ဖုန်းပြောဆိုမှုသည် မလုံခြုံပါ
- SMS ပို့ဆောင်မှုသည် မလုံခြုံပါ
- မဖြစ်မနေ အရေးပေါ်သုံးစွဲရမည်ဆိုပါက Silence SMS (တွဲဖက် လမ်းညွှန်တွင်ပါဝင်သည်) သို့မဟုတ် codeword များသုံးသင့်သည် (ကြိုတင်ပြင်ဆင်ညှိနှိုင်းမှု)
- အလွယ်တကူ လွှင့်ပြစ်၍ ရနိုင်သော မှတ်ပုံတင်ထားခြင်း မရှိသော ကီးပတ်ဖုန်းဝယ် ယူ၍ ပြင်ဆင်ထားပါ (အရေးပါသော contact များ မှတ်ထားပါ၊ အသုံးမပြုပါက battery ဖြုတ်ထားပါ)

လုံခြုံစွာ အင်တာနက်သုံးစွဲခြင်း

- ထိရှလွယ်သော အချက်အလက်များ ပို့ဆောင်ရန် ၊ ဝက်ဆိုက်များ ဝင်ကြည့်ရန် VPN အသုံးပြုပါ
- VPN သည် ဆင်ဆာလုပ်ထားသော website များကိုပါ ကျော်ဖြတ်ကြည့်ရှုနိုင်သည်။
- အခမဲ့အသုံးပြုနိုင်သည့် Psiphon ကို ဤလင့် တွင်ရယူနိုင်ပါသည်။
- အလားတူပင် TOR browser ကိုအသုံးပြု၍ TOR Network ကနေဆင့်လှည့်ပတ်ရောက်ပြီးမှသာ မိမိသွားလိုသည့် Website ကိုကြည့်ရှုပေးသည့်အတွက် မိမိ၏ identity/ location / ISP တို့ကို ကာကွယ်ပေးမည်ဖြစ်သည်။
- ဤ လင့် တွင်သွားရောက်၍ ရယူသုံးစွဲနိုင်ပါသည်။
- သတိပြုရန်မှာ TOR Network အား အသုံးပြုနေကြောင်း ISP ခေါ် အင်တာနက် ကုမ္ပဏီများမှသိရှိနိုင်ပါသည်။
- မိမိသုံးစွဲနေသည့် Operation System (Windows, MaC OS) update များပြုလုပ်ပေးပါ။ Out of date Version များကို သုံးစွဲခြင်းရှောင်ကြည်ပါ။ ဥပမာ Windows XP, Windows 7 ကိုတို့ကို ဆက်လက်သုံးစွဲခြင်းရှောင်ကြည်ပါ။
- မိမိကွန်ပျူတာတွင် Anti-Malware တစ်ခုခုရယူသုံးစွဲပါ အခမဲ့ရယူနိုင်တဲ့ Malwarebytes ကို ဒီနေရာ တွင်ရယူနိုင်ပါသည်။

အချက်လက်များသိမ်းဆည်းခြင်း

- မိမိဖုန်း (သို့) ကွန်ပြုတာ၏ Local Storage ဖြစ်သော Gallery/ File Manager / Device Storage များထဲတွင်ရှိမနေစေရန် အရေးကြီးသည်။
- Encrypt ပြုလုပ်ရမည်။
- ဖုန်းအတွက် Tella Application ကိုအသုံးပြု၍ ဓါတ်ပုံ နှင့် ဗွီဒီယိုမှတ်တမ်းများ လွယ်ကူစွာနှင့် လုံခြုံစွာ သိမ်းဆည်းထား နိုင်သည်။
- ကွန်ပြူတာ နှင့် အခြား storage device များအတွက် VeraCrypt အသုံးပြု၍ (တွဲဖက်ပါ လမ်းညွှန်ကို ဖတ်ရှုနိုင်) encrypt ပြုလုပ်နိုင်ပါသည်။
- Google Drive / Mega ကဲ့ သို့ Online/Cloud ဝန်ဆောင်မှုများ အသုံးပြုပြီး upload လုပ်ကာ sign out ပြုလုပ်နိုင်သည်။

ညှိနှိုင်းမှုပြုလုပ်ခြင်း နှင့် အထွေထွေ

- ခေါ်သော buddy system အားပြင်ဆင်ထားသင့်သည်။
- မိမိတွင် အန္တရာယ် တစ်စုံတရာကျရောက်ပါက ညှိနှိုင်း ဆက်သွယ် ဖြေရှင်းမှုပေးနိုင်သည့် crisis team (အရေးပေါ် တုံ့ပြန်ရေး အဖွဲ့) စတင်စီစဉ်ထားရမည်
- လက်ပြောင်းလွှဲရေး (Handover) အစီစဉ် ဖော်ဆောင်ထားရမည်
- ဖုန်းအပို ရှာဖွေထားရမည်
- မိမိတစ်ကိုယ်ရည် အသုံးအဆောင် များအား သယ်ယူရန် လွယ်ကူသည့် ကျောပိုးအိတ် (သို့) ခရီးဆောင်အိတ်ပြင်ဆင်ထားရမည်

- မိမိတို့၏ ဒစ်ဂျစ်တယ် ပိုင်ဆိုင်မှုများအား ထိရှလွယ်နိုင်မှုအဆင့် sensitivity level နှင့် လုပ်ဆောင်ရမည့် အဆင့်များကို စီစစ်၍ ဆောင်ရွက်ရန်ကိစ္စများကို စီစဥ်ဖော်ထုတ်ပါ။ (ထိုအတွက် တွဲဖက်ပါ Self Help Mapping အသုံးပြု၍ စီစဥ်ပါ)
- Keepass ဖိုင် အဆင်သင့်ပြင်ထားပါ။

CODE YELLOW

ဤလမ်းညွှန် သည် စိုးရိမ်ဖွယ် ရေချိန်အရ ပြင်ဆင်ထားသင့်သော၊ ပုံမှန်ကျင့်သုံးသင့် သောဒစ်ဂျစ်တယ် လုံခြုံရေး အမူအကျင့်များနှင့် ပြင်ဆင်ထားသင့်သည်များကို ပြုစုထားသော လမ်းညွှန်တစ်ခုဖြစ်သည်။ CODE YELLOW (အဝါရောင်အဆင့်) ဟု သတ်မှတ်သည့် အခြေအနေများ တွင် မိမိ၏ ဒစ်ဂျစ်တယ် လုံခြုံရေးအား “ကြိုတင်ကာကွယ်” ထားနိုင်ဖို့ ရည်ရွယ်သည်။

Code Yellow ဆိုသည်မှာ

- **အင်တာနက်ရရှိနေချိန်**
- **မိမိအားပစ်မှတ်အဖြစ် သတ်မှတ်ခံရထားတော့မည်ကိုသိနှင့်နေသောအချိန် (သို့) ဖမ်းဆီးထိန်းသိမ်းခံရနိုင်မှု အမြင့်ဆုံးနှင့် ဖမ်းဆီးခံရချိန်**
- **မိမိ၏ ဒစ်ဂျစ်တယ် ပစ္စည်းများကို လုံခြုံရေးတိုးမြှင့်ဖို့ရန်အတွက် အချိန်လုံလောက်စွာမရတော့ချိန်တို့တွင်**

တို့တွင် ဆက်သွယ်လုပ်ဆောင်မှုများ လုံခြုံ စေရန် သတိပြုလိုက်နာသင့်သော အကြံပြုချက်များဖြစ်သည်။

အင်တာနက်ပြတ်တောက်သွားပြီး မိမိ ကိုယ်ကိုသော်လည်းကောင်း မိမိအဖွဲ့အစည်းကိုသော် လည်းကောင်း ပစ်မှတ်ထားခံရမှု အမြင့်ဆုံးဖြစ်နေသည်ဟု ယူဆရသည့် အချိန်တွင် CODE RED လမ်းညွှန်များအား ထပ်မံဖတ်ရှုသင့်သည်

ဤလမ်းညွှန် သည် မိမိနှင့် မိမိအဖွဲ့အစည်းကို ပစ်မှတ်ထား ဖမ်းဆီးထိန်းသိမ်းခြင်း(သို့မဟုတ်) တိုက်ခိုက်ခြင်းတို့ ခံရနိုင်ချေ အမြင့်ဆုံးအချိန်တွင် ဒစ်ဂျစ်တယ်လုံခြုံရေးဆိုင်ရာပြင်ဆင်မှုများ ဆောင်ရွက်နိုင်ရန် အချိန်နည်းပါးနေချိန်တွင် လုပ်ဆောင်ရမည့် အရေးပေါ်အခြေအနေဖြစ်ပါသည်။

မိမိ အဖမ်းခံရပြီ၊ တိုက်ခိုက်ခံရပြီဆိုလျှင် ထိုသို့တိုက်ခံရကြောင်း ဖမ်းဆီးခံရကြောင်းကို မိမိ၏ network မှ လူများ အမြန်ဆုံးသိရှိနိုင်အောင် ဆောင်ရွက်ရန်ဖြစ်ပါသည်။

Code Yellow ဟု ယူဆရသည့် အချိန်၊ အဖမ်းခံ ရခြေရှိသည့် အခြေအနေဆိုလျှင်အရင်ဆုံး

- မိမိ၏ ဖုန်းနှင့်ကွန်ပြူတာ၊ Tablet အတွင်းရှိ ဒေတာအချက်အလက်များအား တစ်နေရာထဲတွင် စုစည်း Backup လုပ်ပါ။
- ဖုန်း contact များကို export ထုပ်ပြီး backup လုပ်ပါ။
- Password manager အသုံးပြုပြီး Password များသိမ်းထားသည့် ဖိုင်အား Backup လုပ်ပါ။

- ဆက်သွယ်ပြောဆိုသည့် ကြားခံ Application များကို Messenger ကဲ့သို့ မလုံခြုံသည်ကို အသုံးမပြုဘဲ Signal, Telegram ကဲ့သို့ End to End Encryption ပါသည့် ဆက်သွယ်ရေး App များကိုသုံးနေသင့်ပါသည်။
- မုချ အဖမ်းမခံမီ ဆက်ကြားတွင် မိမိ ၏ဖုန်းများ Factory Format ချရန်လိုအပ်ပါသည်။ Factory Format ချရန်အတွက် အချိန် (10−20) မိနစ်ကြာနိုင်ပါသည်။ iphone နှင့် Xaiomi ဖုန်းများကိုင်ဆောင်ထားသောသူများသည် iCould (သို့) MiCloud တို့ထဲမှာလည်း Sign Out ထွက်ပေးရန်လိုအပ်ပါသည်။
- မိမိ ၏ Password file အား အသက်လဲပြီး ယုံကြည်ရသူကို Master Password ပေးထားခဲ့ပါ။

Internet ပြတ်တောက် မခံရခင် ပြုလုပ်နိုင်သော ကြိုတင်ပြင်ဆင်မှုများ

- Internet ပြတ်တောက်ခံရခြင်းသည် အခြေအနေအမျိုးမျိုးတွင် ဖြစ်နိုင်သောကြောင့် အဝါရောင် အဆင့်သည် မိမိအဖွဲ့အစည်း (သို့) မိမိ၏ ဆက်သွယ်ရေး အတွက် ဒီအဆင့်တွင် ကြိုတင်ပြင်ဆင်မှုများ ပြုလုပ်ထားသင့်သည်။

CODE RED

ဤလမ်းညွှန် သည် စိုးရိမ်ဖွယ် ရေရှိန်အမြင့်ဆုံးရောက်ရှိချိန်တွင် လုပ်သင့်သည်ဟု ယူဆရသော မိမိကိုယ်ကို ကာကွယ်နိုင်မည့်၊ ဆက်သွယ်ရေးမပြတ်စေရန် လုပ်ဆောင်နိုင်မည့် လုပ်ငန်းဆောင်တာများအား စုစည်းထားခြင်းဖြစ်သည် ။ CODE RED (အနီရောင်အဆင့်) ဟု သတ်မှတ်သည့် အခြေအနေများ တွင် တတ်နိုင်သမျှ လုပ်ရှားဆောင်ရွက်နိုင်ဖို့ ရည်ရွယ်သည်။

Code Red ဆိုသည်မှာ

- **အင်တာနက်ပြတ်တောက်သွားသည့်အချိန်**
- **မိမိ၏အချက်အလက်များကို လုံခြုံစွာ ဆက်လက်ရှိနေစေဖို့ အပြင်အင်တာနက်ပြတ်တောက်သွားပါက မိမိအဖွဲ့အစည်းများအကြား ဆက်သွယ်ရေး Channel များကြိုတင်ပြင်ဆင်ထားရမည့် အရာများအတွက် အ
  အကြံပြုချက်များဖြစ်သည်။**

အင်တာနက်မရှိသည့် (အင်တာနက်ဖြတ်တောက်ခံထားရသည့်) အချိန်တွင် တစ်ဦးနှင့်တစ်ဦး လုံခြုံစွာ ဆက်သွယ်နိုင်ရေးသည် အလွန်စိန်ခေါ်မှု ကြီးမားသည့် အခြေအနေဖြစ်သည်။ ဖုန်းနှင့်ဖြစ်စေ စာတိုပို့စနစ်နှင့်ဖြစ်စေ ဆက်သွယ်မှုသည် ကြားမှဖြတ်ယူနားထောင် ဖမ်းယူရရှိနိုင်ကြောင်း သတိမူရမည် ဖြစ်သည်။

ဤအခြေအနေတွင် Andriod ဖုန်း အသုံးပြုသူများကြား အချင်းချင်း လုံခြုံစွာ စာတိုပေးပို့နိုင်ရန်အတွက် [Silence application](#) ကိုအသုံးပြုရန် အကြံပြုပါသည်။ အခြား ဝန်ဆောင်မှု နှင့် နည်းပညာများသည် အင်တာနက် အပေါ်မှီခိုရသောကြောင့် ဤကဲ့သို့ အင်တာနက်ဖြတ်တောက်ခံရသည့် အခြေနေများ၌ မိမိ၏ အချက်လက်ဆိုင်ရာ လုံခြုံမှုသည် မိမိ၏ အပြုအမူ/ကြံစည်မှုများ အပေါ်လည်း မူတည်နိုင်ပါသည်

။ ဥပမာအားဖြင့် သွယ်ဝိုက်၍ စကားဝှက် (codewords) များကိုအသုံးပြုခြင်းအပြင် အခြား မိမိတို့ အသုံးပြုနေကျ အချက်ပြမှုများကိုလည်း သုံးစွဲနိုင်ပါသည်။

Documentation

အင်တာနက် မရှိချိန်တွင် Documentation ပြုလုပ်ရန်အတွက် Tella Application ကိုအသုံးပြု၍ ဓါတ်ပုံ နှင့် ဗွီဒီယိုမှတ်တမ်းများ လွယ်ကူစွာနှင့် လုံခြုံစွာ သိမ်းဆည်းထား နိုင်သည်။

အင်တာနက်မရှိချိန် ဆက်သွယ်ခြင်း

အင်တာနက်မရှိချိန်တွင် အဆက်အသွယ် လုပ်ဖို့ရာအတွက် များသောအားဖြင့် Briar, Bridgefy, Talkie အစရှိသည့် Bluetooth သို့မဟုတ် NFC တို့ကို အသုံးပြု၍ ဆက်သွယ်သော နည်းလမ်းများရှိသည်။ ချိတ်ဆက်သူများပြားလာသည်နှင့်အမျှ ဆက်သွယ် နိုင်သည့် ဧရိယာမှာလည်းပိုမိုကျယ်ပြန့်လာမည်ဖြစ်သည်။ များသောအားဖြင့် ဆန္ဒပြပွဲများတွင် အသုံးများသည်။ သို့သော် အနီးအနားတွင်ရှိသမျှ အသုံးပြုသူများဝင်လာနိုင်သည်ဖြစ်၍ လုံခြုံရေးအရ ပြဿနာရှိနိုင်သည်ကို သတိပြုသင့်သည်။

Low-Cost Mesh Network (wifi bridging)

အင်တာနက်ဖြတ်တောက်ခံရသည့် အချိန်တွင် တစ်ယောက်နှင့်တစ်ယောက် ဆက်သွယ်နိုင်ရန် နည်းလမ်းနှစ်မျိုးရှိပါသည်။

- Local area
- Long range area (budget mesh)

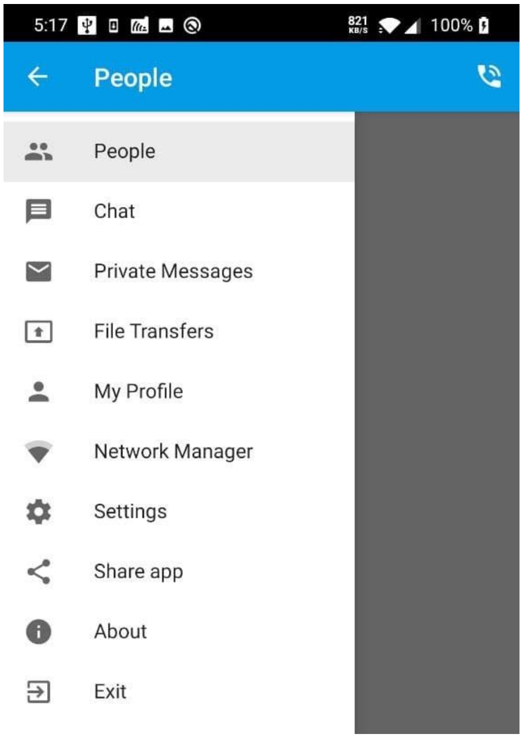
Local Area ဆိုသည်မှာ အနီးဝန်းကျင်အတွင်း ဆက်သွယ်ရန် Router, Ananda စက်, Portable hotspot ထောင်နိုင်သော စက် စသည့် wifi ချိတ်ဆက်နိုင်သော စက်များ လိုအပ်ပါသည်။ တစ်ယောက်က Hotspot ထောင်ပြီး တစ်ခြားစက်များက လာရောက်ချိတ်ဆက်ခြင်းဖြစ်ပါသည်။ ပြီးလျှင် အောက်တွင်ဖော်ပြထားသည့် App ကိုအသုံးပြု၍ စတင်ချိတ်ဆက် စကားပြောနိုင်ပြီဖြစ်သည်။

Long Range Area ဆိုသည်မှာ အထက်ပါ Local area ပုံစံအတိုင်း သို့သော် Router ကို extend လုပ်ပြီး network ကိုဝေးဝေး ရောက်အောင် လုပ်ဆောင်ခြင်း ဖြစ်သည်။

App သည် Android အတွက်သာဖြစ်သည်။ Computer အချင်းချင်း ချိတ်ဆက် စကားပြောနိုင်ရန် ->
Lan Messenger -> http://lanmsngr.sourceforge.net/

Talkie
For Android only
https://play.google.com/store/apps/details?id=com.remaller.android.wifitalkie_lite&hl=en&gl=US

Zapya ကို လူတိုင်း သိကြမယ်လို့ထင် ပါသည်။ အဆိုပါ App ၏ အလုပ်လုပ်နှင့် အတူပင်ဖြစ်ပါသည်။



People -> အနီးအနားရှိ Talkie အသုံးပြုသူများအားကြည့်ရန်
Chat -> အနီးအနားရှိ Talkie အသုံးပြုသူများ နှင့်စကားပြောရန်
Private Messages -> အနီးအနားရှိ Talkie အသုံးပြုသူများ နှင့်တိုက်ရိုက် စကားပြောရန်
File Transfers -> အနီးအနားရှိ Talkie အသုံးပြုသူများ နှင့် ဖိုင်များ ရှဲရန်
My Profile -> မိမိ၏ Profile အား ပြင်ဆင်ရန်
Network Manager -> Hotspot ထောင်ခြင်း နှင့် ရှိပြီးသား wifi network အားချိတ်ဆက်ရန်