EFF'S SURVEILLANCE SELF-DEFENSE

စကားဝှက်သော့ စစ်ဆေးအတည်ပြုခြင်း

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

LOCALIZATION LAB

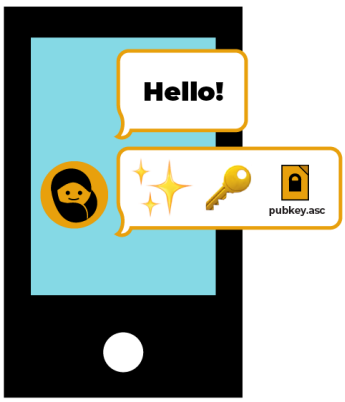
စကားဝှက်သော့ စစ်ဆေးအတည်ပြုခြင်း

ကုဒ်ဖြင့်ပြောင်းလဲခြင်း အကြောင်း နားလည် သိရှိထားခြင်းမရှိလျှင် ကုဒ်ဖြင့်ပြောင်းလဲခြင်း၏ အဓိက အယူအဆများ ကို အရင်ဖတ်ပါ။

အစ-အဆုံးကုဒ်ဖြင့်ပြောင်းလဲခြင်းကို အသုံးပြုပြီ အွန်လိုင်းပေါ်တွင် ဆက်သွယ်မှုများ ပြုလုပ်သည့် အခါမှာ သင်မက်ဆေ့ချ် ပေးပို့ ဆက်သွယ်သူ တစ်ဦးချင်းစီမှာ တခြားသူနဲ့မတူတဲ့ ကိုယ်ပိုင်အများသုံး စကားဝှက်သော့ ရှိပါတယ်။ သူတို့ဆီပို့တဲ့မက်ဆေ့ချ်ကို ကုဒ်နဲ့ပြောင်းလဲတဲ့အခါ အဲဒီသော့ကို သုံးရပါ တယ်။ ဒါမှ ကာယကံရှင်ပဲ မက်ဆေ့ချ်ကို ပြန်ဖြည်နိုင်မှာပါ။

သင့်အနေနဲ့ ဘယ်အများသုံးသော့ကို သုံးရမလဲဆိုတာ ဘယ်လိုသိနိုင်မလဲ။

သင့်သူငယ်ချင်း အက်စ်ရာဆီက လို့ပြောတဲ့ အီးမေးလ်တစ်ခုကို သင်လက်ခံရရှိတယ်ဆိုပါစို့။ ဒီအီးမေးလ်ထဲမှာ နောင်အခါ မက်ဆေ့ချ်တွေကို လုံလုံခြုံခြုံပို့ဖို့သုံးနိုင်မယ့် PGP အများသုံး ဝှက်စာသော့ဖိုင် တစ်ခု ပါနေတယ်ဆိုပါစို့။ ဒါမှမဟုတ် သင့်သူငယ်ချင်း အက်စ်ရာဆိုပြီး ကုဒ်ဖြင့်ပြောင်းလဲခြင်းကို အသုံးပြုတဲ့ မက်ဆေ့ချ်ပို့နိုင်တဲ့ အက်ပလီကေးရှင်းတွေဖြစ်တဲ့ WhatsApp၊ Signal (သို့) Wire က တဆင့် ကုဒ်ဖြင့်ပြောင်းလဲနိုင်တဲ့ လုံခြုံရေးကုဒ်ကိုပေးပို့ပြီး ချက်တင်လုပ်ဖို့လာတောင်းဆိုမယ် ဆိုပါစို့။



စမတ်ဖုန်းပေါ်မှာ သင့်သူငယ်ချင်း အက်စ်ရာဆီက လို့ပြောတဲ့ မက်ဆေ့ချ်ကို တွေ့နိုင်ပါတယ်။ သူမက “ဟဲလို” လို့မက်ဆေ့ချ်ပို့ပြီးတာနဲ့ အများသုံးဝှက်စာသော့ (pubkey.asc) နဲ့ အီမိုဂျီတွေပါတဲ့ မက်ဆေ့ ထပ်ပို့ပါတယ်။

ဒီမက်ဆေ့ချ်တွေက အက်စ်ရာဆီကလာတာ ဟုတ်ချင်မှ ဟုတ်ပါမယ်။

သင့်အနေနဲ့ အက်စ်ရာရဲ့ အများသုံးသော့ကို သုံးနေတယ်လို့ ထင်ရပေမယ့် တကယ်တမ်းကျတော့ အခြားတစ်ယောက်က ဟန်ဆောင်ပို့လိုက်တဲ့ အများသုံးသော့ကို သုံးနေရတာဖြစ်နိုင်တယ်။ ဆိုလိုတာက အက်စ်ရာမဟုတ်တဲ့ တစ်ယောက်က သင်ပို့တဲ့မက်ဆေ့ချ်တွေကို ပြန်ဖြည်လို့ရတယ် ဆိုတာပါပဲ။

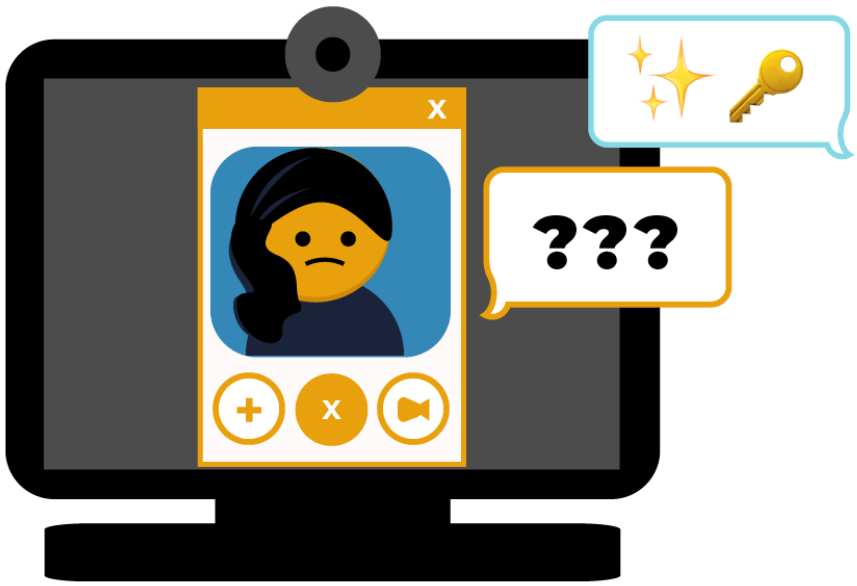
သင့်အနေနဲ့ မှန်ကန်တဲ့ စကားဝှက်ကို အသုံးပြုနေတာဟုတ်၊ မဟုတ် နဲ့ (သူများတွေက သင့်စကားဝှက်သော့မှန်၊မမှန်) စစ်ဆေးဖို့ အတွက် စကားဝှက်သော့အတည်ပြုခြင်းကို လုပ်ဆောင်ဖို့လိုပါတယ်။

စကားဝှက်သော့ အတည်ပြုခြင်းကို ဘယ်အချိန်၊ ဘယ်နေရာမှာ လုပ်ဆောင် သင့်သလဲ။

စကားဝှက်သော့ အတည်ပြုဖို့ရာ မတူညီတဲ့ မက်ဆေ့ချ်ပို့တဲ့ စနစ်တွေအတွက် မတူညီတဲ့နည်းလမ်းတွေ ရှိပါတယ်။ အကုန်လုံးမှာ တူညီတာတစ်ခုက မက်ဆေ့ချ်ပို့တဲ့စနစ်ကို မသုံးဘဲ အတည်ပြုရတာပါ။ အဲဒါကို စနစ်ပြင်ပအတည်ပြုခြင်းလို့ ခေါ်ပါတယ်။ သင့်အနေနဲ့ အွန်လိုင်းပေါ်က အက်စ်ရာနဲ့ အပြင်က အက်စ်ရာဟာ တစ်ယောက်တည်းဖြစ်ကြောင်း စစ်ဆေးရပါမယ်။ ဒီလိုလုပ်ဖို့ အက်စ်ရာ့ဆီဖုန်းခေါ်တာပဲဖြစ်ဖြစ်၊ လူချင်းတွေ့ပြီးပဲဖြစ်ဖြစ် သင့်ဆီပို့လိုက်တဲ့ အများသုံး စကားဝှက်သော့ဟာ သူ့ဆီကဖြစ်ကြောင်း အတည်ပြုနိုင်ပါတယ်။

စနစ်ပြင်ပအတည်ပြုခြင်း ကို ဘာကြောင့်လုပ်သင့်သလဲ?

- စကားဝှက်သော့ကို ဘယ်သူ့ဆီက ပို့သလဲဆိုတာကို အတည်ပြုမထားရင် လုံခြုံရေး ဝှက်စာပေးပို့မှု စနစ်က မလုံခြုံတော့ဘူးလို့ ဆိုနိုင်ပါတယ်။
- အက်ပလီကေးရှင်းတိုင်း၊ ဝန်ဆောင်မှုတိုင်းမှာ အခြားသူတစ်ယောက်လို ဟန်ဆောင်ဖို့ ခက်ခဲပါတယ်။ ဥပမာအားဖြင့် သင်က Signal လက်ဗွေကို FaceTime ဗီဒီယိုချက်တင်နဲ့ အတည်ပြုမယ်ဆိုရင် သင့်သူငယ်ချင်း ဟန်ဆောင်တဲ့သူဟာ Signal အကောင့်ရော၊ FaceTime အကောင့်ရောအတွက် အကောင့်တုတွေ လုပ်ထားဖို့ ခက်ပါလိမ့်မယ်။ ပြီးတော့ ဗီဒီယိုမှာလည်း မျက်နှာကို တွေ့ရတာမို့ သင့်သူငယ်ချင်းလို ဟန်ဆောင်ဖို့ ပိုခက်ပါတယ်။

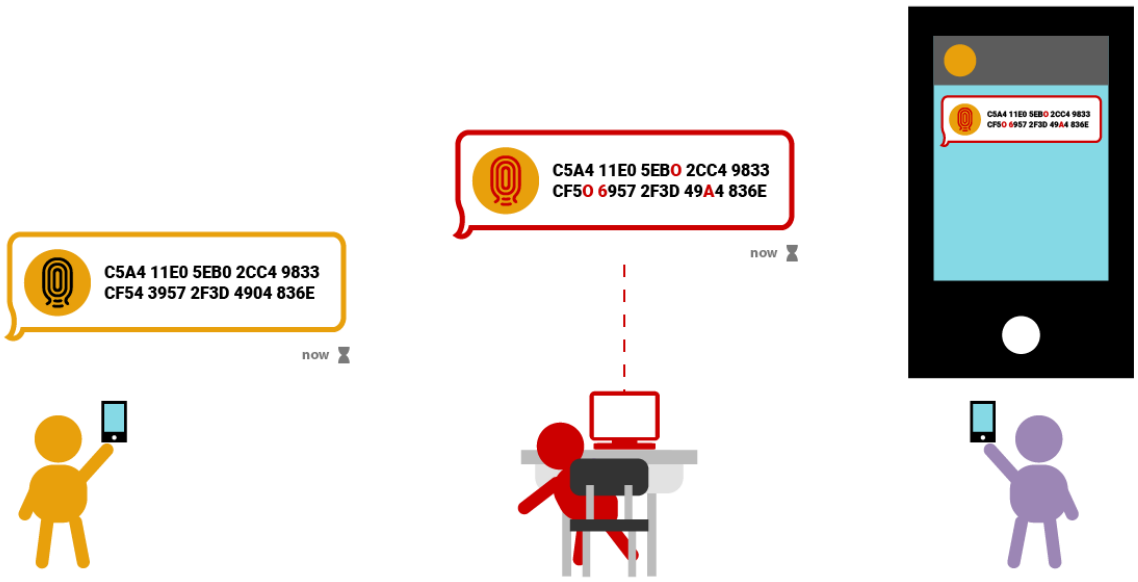


Signal တွင် ပေးပို့လိုက်သည့် စကားဝှက်သော့ကို ဗွီဒီယိုကောလ်ဖြင့် အတည်ပြုခိုင်းသည့် အတွက် စိတ်ပူပန်နေပုံ။

သင့်အတွက် မရှင်းမလင်းဖြစ်မယ်လို့ထင်တဲ့ အချက်တစ်ချို့ကို ဖော်ပြပေးလိုက်ပါတယ်။

မေးခွန်း- အက်စ်ရာကို အွန်လိုင်းကနေပဲ မေးခွန်းတွေမေးပြီး စစ်ဆေးအတည်ပြုလို့မရဘူးလား။ ဥပမာအားဖြင့် "နင်က အက်စ်ရာအစစ်ဆိုရင် ငါတို့နောက်ဆုံးတွေ့တုန်းက ဘာဝတ်ထားလဲ" ဆိုတဲ့ မေးခွန်းမျိုးပေါ့။

အဖြေ- ပြဿနာက သင်နဲ့စကားပြောနေတဲ့ အက်စ်ရာအတုက တချိန်တည်းမှာပဲ သင့်ဟန်ဆောင်ပြီး အက်စ်ရာအစစ်နဲ့ စကားပြောနေနိုင်ပါတယ်။ ဒီလိုဆိုတော့ သင်မေးတဲ့မေးခွန်းတွေကို အက်စ်ရာအစစ်ကို မေးပြီး သင့်ဆီကို အဖြေမှန်တွေပြန်ပို့နိုင်တာပေါ့။ အဲဒီလိုလုပ်တာကို ကြားခံလူ/စက်မှ တိုက်ခိုက်ခြင်းလို့ခေါ်ပါတယ်။ ဒီလိုမျိုး ရံဖန်ရံခါဖြစ်တတ်တာမို့ စကားဝှက်သော့ အတည်ပြုတဲ့အခါ စနစ်ပြင်ပ အတည်ပြုခြင်းကို လုပ်ဆောင်ဖို့ လိုပါတယ်။



စမတ်ဖုန်းတွေကိုင်ထားတဲ့ လူနှစ်ယောက်။ ဘယ်ဘက်လူက သူ့ရဲ့ အများသုံး စကားဝှက်သော့လက်ဗွေကို ချက်တင်ကနေ ပို့လိုက်ပါတယ်။ ညာဘက်လူဆီ မရောက်ခင်မှာပဲ အလယ်မှာရှိတဲ့ လူက ပေးပို့သူရဲ့ မက်ဆေ့ချ်ကို ကြားဖြတ်ယူပြီး လက်ဗွေမှာ ပါရှိတဲ့ ကိန်းဂဏန်းနဲ့စာလုံး အချို့ကို အပြောင်းအလဲလုပ် လိုက်ပါတယ်။ ပြီးတော့မှ ညာဘက်က လက်ခံသူဆီပို့ပေးလိုက်ပါတယ်။ ညာဘက်မှာ လက်ခံသူရဲ့ဖုန်းကို ပြထားပါတယ်။ မက်ဆေ့ချ်က မူလပေးပို့သူဆီက လာသလိုထင်ရပေမယ့် တကယ်တမ်းကျတော့ ကြားလူရဲ့စနက်နဲ့ လိမ်ထားတဲ့ မက်ဆေ့ချ် အတုကြီးဖြစ်နေပါတယ်။

မေးခွန်း- မိမိနဲ့ ဆက်သွယ်သူဟာ လူလိမ်မဟုတ်ဘဲ အစစ်အမှန်ဖြစ်ကြောင်း သေချာနေရင်ရော ဝှက်စာသော့ကို အတည်ပြုစစ်ဆေးဖို့ လိုသေးလား။

အဖြေ- ဝှက်စာသော့ကို ယုံကြည်ရတဲ့ သူဆီက ရတယ်ပဲထားပါတော့။ ဘယ်လောက်ပဲ သေချာပါစေ သော့ကို အတည်ပြုစစ်ဆေးတာက မှန်ကန်တဲ့လုပ်ရပ် ဖြစ်ပါတယ်။ ဒီလိုလုပ်ခြင်းအားဖြင့် သင့်တို့ အပြန်အလှန်ပေးပို့မယ့် မက်ဆေ့ချ်တွေရဲ့ လုံခြုံမှုကို ဂရုစိုက်ရာ ရောက်ပါတယ်။

မေးခွန်း- ဘယ်အချိန်မှာ စကားဝှက်သော့ကို အတည်ပြုစစ်ဆေးသင့်သလဲ။

အဖြေ- သင့်အနေနဲ့ မက်ဆေ့ချ်ပို့တဲ့ အက်ပ်အသစ်ကို စသုံးတာပဲဖြစ်ဖြစ်၊ သင်နဲ့ ဆက်သွယ်သူတစ်ဦးဦးရဲ့ စကားဝှက်သော့ ပြောင်းသွားတာပဲဖြစ်ဖြစ်- အဲဒီအချိန်မျိုးမှာ စစ်ဆေးအတည်ပြု သင့်ပါတယ်။ အောက်မှာတော့ စကားဝှက်သော့ပြောင်းလဲသွားနိုင်တဲ့ အခြေအနေတချို့ကို ဖော်ပြပေးထား ပါတယ်။

- PGP အသုံးပြုသူရဲ့ ဝှက်စာသော့ သက်တမ်း ကုန်ဆုံးသွားတာ ဖြစ်နိုင်ပါတယ်။
- ဖုန်းနဲ့မက်ဆေ့ချ်ပို့ရတဲ့ အက်ပ်အချို့က စကားဝှက်သော့ကို ဖုန်းနဲ့ တွဲထားတတ်ပါတယ်။ အသုံးပြုသူက ဖုန်းအသစ်ဝယ်တဲ့အခါ စကားဝှက်သော့အသစ်ပြောင်းရတတ်ပါတယ်။
- တခါတလေမှာ စကားဝှက်သော့ပျောက်တာမျိုး (သို့မဟုတ်) သော့ကိုဖွင့်တဲ့ စကားဝှက်တွေ ကို မေ့တာမျိုးကြောင့်လည်း ဖြစ်နိုင်ပါတယ်။

ဘယ်လိုပဲဖြစ်ဖြစ် စကားဝှက်သော့ အသစ်ပေးပို့လာတာနဲ့ အတည်ပြုစစ်ဆေးသင့်ပါတယ်။

ဒါဆိုရင် ဒီသော့တွေကို ဘယ်လိုစစ်ဆေးကြမလဲ။

စနစ်ပြင်ပတွင် ဝှက်စာသော့များအား စစ်ဆေးအတည်ပြုခြင်း

ကုဒ်ဖြင့်ပြောင်းလဲခြင်း အတွက် အသုံးပြုတဲ့ စကားဝှက်သော့တွေဟာ တကယ်တော့ အလွန်ရှည်လျားတဲ့ ကိန်းစဉ်တွဲများ ဖြစ်ပါတယ်။ အဲဒီကိန်းဂဏန်းတွေကို နူတ်တိုက်အော်ဖတ်ပြီး စစ် ဆေးဖို့ဆိုတာ ခက်ပါတယ်။ အဲဒီလိုအခြေအနေမှာ ဆော့ဖ်ဝဲကိုသုံးပြီးသော့ကို အတည်ပြုလို့ ရပါတယ်။ အဲဒီဆော့ဖ်ဝဲလ်က စကားဝှက်သော့ကို အခြေခံထားတဲ့ လက်ဗွေ (သို့မဟုတ်) လုံခြုံရေးလျှို့ဝှက်နံပါတ်ကို ထုတ်ပေးနိုင်ပြီး အလွယ်တကူ စစ်ဆေးအတည်ပြုလို့ ရစေပါတယ်။ လက်ဗွေလို့ ဆိုတဲ့နေရာမှာ သေးငယ်တဲ့ ကိန်းဂဏန်း (သို့မဟုတ်) စကားလုံးအတွဲလိုက် (သို့မဟုတ်) ပုံတစ်ပုံ ဖြစ်နိုင်ပါတယ်။

စကားဝှက်သော့ကို အတည်ပြုဖို့အတွက် သူတို့ရဲ့ သော့ကို ဖတ်ပြတာ (သို့မဟုတ်) ထုတ်ပြတဲ့အခါ သင့် စက်မှာရှိတဲ့ သူတို့ပေးပို့ထားတဲ့ လက်ဗွေနဲ့ တိုက်ဆိုင်စစ်ဆေးဖို့ လိုပါမယ်။ သူတို့ရဲ့ သော့ကို စစ်ဆေး အတည်ပြုပြီးတဲ့အခါ သင့်သော့ကိုလည်း အတည်ပေးဖို့လိုပါတယ်။ သင့်ရဲ့ စကားဝှက်သော့လက်ဗွေ ကိုဖတ်ပြတာ (သို့မဟုတ်) ထုတ်ပြတဲ့အခါ သူတို့စက်ထဲမှာရှိတာနဲ့ တိုက်စစ်ပါလိမ့်မယ်။ နှစ်ဖက်လုံးတိုက်စစ်ပြီးလို့ မှန်ကန်တယ်ဆိုရင် သင်တို့နှစ်ယောက် လုံလုံခြုံခြုံ ဆက်သွယ်လို့ ရပြီပေါ့။

စနစ်ပြင်ပ စစ်ဆေးအတည်ပြုနိုင်တဲ့ နည်းလမ်းတွေအများကြီးထဲက အများဆုံးသုံးတဲ့ နည်းလမ်းတွေ ကိုဖော်ပြပေးသွားပါမယ်။

(၁) လူချင်းတွေ့၍ စစ်ဆေးအတည်ပြုခြင်း (သို့မဟုတ်)

(၂) သင်တို့အသုံးပြုနေတဲ့ စနစ်မဟုတ်တဲ့ အခြားစနစ်တစ်ခုခုကို သုံးပြီး အတည်ပြုခြင်း

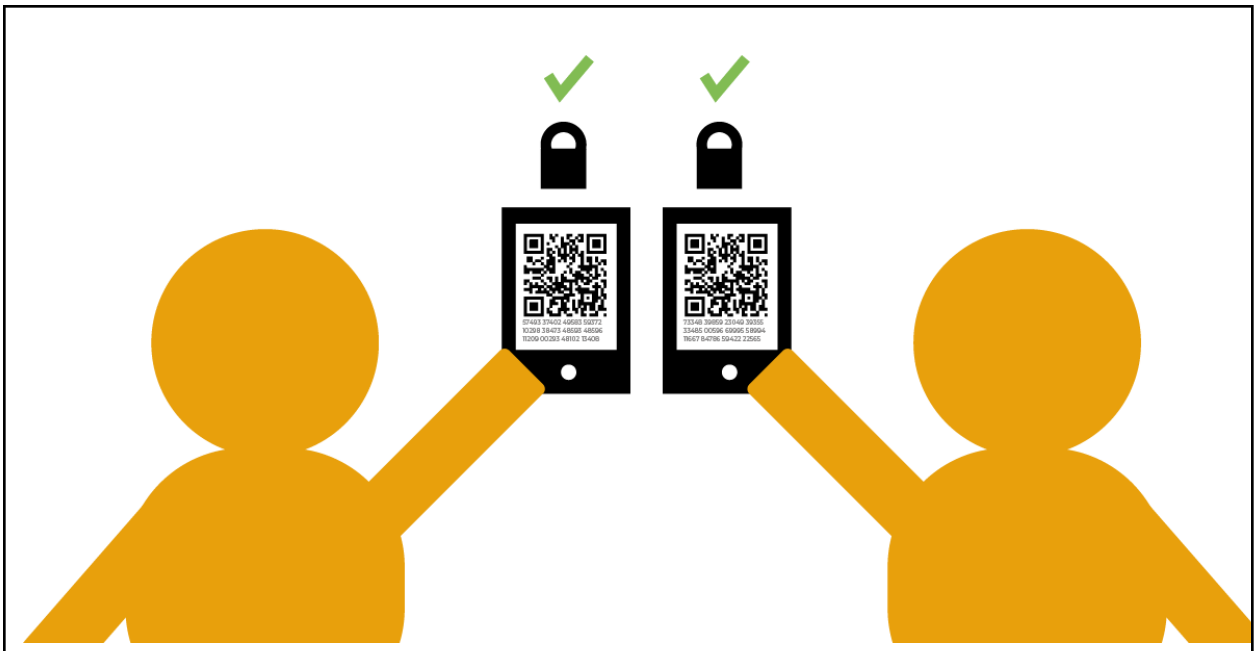
လူချင်းတွေ့၍ စစ်ဆေးအတည်ပြုခြင်း

အကောင်းဆုံးက လူချင်းတွေ့ပြီးစစ်ဆေး အတည်ပြုတာပါပဲ။ အဲဒီ လူဟုတ်၊ မဟုတ်ဆိုတာကို ဟန်ဆောင်တာ/ ဖစ်ရှင်းလုပ်တာမျိုးတွေ တွေ့ကြုံနိုင်တဲ့) ချက်တင်၊ အီးမေးလ်နဲ့ ဆိုရှယ်မီဒီယာ ချက်တင် စတာတွေကတဆင့် စစ်ဆေးခြင်းထက် လူချင်းမျက်နှာချင်းဆိုင်တွေ့တာက အလွယ်ဆုံးနည်းလမ်း ဖြစ်ပါတယ်။

လူချင်းတွေ့တဲ့အခါ သင့်မိတ်ဆွေဆီမှာရှိတဲ့ သင့်ရဲ့အများသုံးဝှက်စာသော့မှာပါတဲ့ စာလုံးတစ်လုံးချင်းစီကို သင့်ရဲ့ အများသုံးဝှက်စာသော့နဲ့ တိုက်ဆိုင်စစ်ဆေးလို့ရပါတယ်။ နည်းနည်းတော့ လက်ပေါက်ကပ်ပေမဲ့ တန်ပါတယ်။ သင်နဲ့သင့်မိတ်ဆွေတို့ အများသုံးစကားဝှက်သော့လက်ဗွေကို လိပ်စာကတ် လဲသလို လဲကြတဲ့အခါ ဒါမှမဟုတ် အစည်းအဝေးမှာတွေ့တဲ့အခါမျိုးမှာ လူချင်းတွေ့တဲ့ နည်းလမ်းကို အသုံးပြု နိုင်ပါတယ်။

အစ-အဆုံးကုဒ်ဖြင့် ပြောင်းလဲခြင်း စနစ်ကိုသုံးထားတဲ့ မက်ဆေ့ချ်အက်ပ်တွေမှာ စကားဝှက်သော့ လက်ဗွေကို စစ်ဆေးအတည်ပြုနိုင်မယ့် နည်းလမ်းတွေ ထည့်သွင်းပေးထားပါတယ်။ အက်ပ်အားလုံးအတွက် ဘုံသုံးတဲ့နည်းလမ်းရယ်လို့တော့ မရှိသေးပါဘူး။ အက်ပ်တစ်ခုအတွက် လက်ဗွေမှာပါတဲ့ စာလုံးတစ်ခုချင်းစီကို ဖတ်ပြီး သင့်မိတ်ဆွေဖုန်းစခရင်နဲ့ တိုက်စစ်ရတာမျိုးဖြစ်နိုင်ပါတယ်။ အခြားအက်ပ်တစ်ခုမှာတော့ စကားဝှက်သော့ကို အတည်ပြုဖို့ သင့်မိတ်ဆွေဖုန်းပေါ်က QR code ကို ဖတ်ရတာမျိုးဖြစ်နိုင်ပါတယ်။

အန်မင်းက သူမရဲ့သူငယ်ချင်း ဂါဆန်နဲ့ပွဲတစ်ခုမှာတွေ့တယ် ဆိုပါစို့။ သူတို့နှစ်ယောက်ကြား [အစ-အဆုံးကုဒ်ဖြင့်ပြောင်းလဲခြင်း](#)ကို သုံးတဲ့ အက်ပ်ကနေ ဆက်သွယ်ဖို့ ဆုံးဖြတ်လိုက်ကြတယ်။ ဒါ့ကြောင့် သူတို့ဖုန်းတွေထဲကို Signal (သို့) WhatsApp ကို ထည့်သွင်းလိုက် ကြပါတယ်။ အန်မင်းနဲ့ ဂါဆန်းတို့ဟာ လူချင်းတွေ့တဲ့အချိန်မှာ ဒီနည်းလမ်းကို သုံးဖို့ဆုံးဖြတ်လိုက်တာမို့ စကားဝှက်သော့ကို အတည်ပြုဖို့ရာ လွယ်ကူသွားပါတယ်။



လူနှစ်ယောက်က QR code တွေနဲ့ ကိန်းစဉ်တွေ စာလုံးတွေပါတဲ့ စာတွဲကြီးတွေပေါ်နေတဲ့ ဖုန်းစခရင်နှစ်ခုကို ယှဉ်လျက်ကိုင်ထားပါတယ်။ တစ်ယောက်နဲ့တစ်ယောက် ဖုန်းကင်မရာသုံးပြီး အပြန်အလှန် QR code စကင်ဖတ်လို့ စကားဝှက်သော့ကို အတည်ပြုကြပါတယ်။ သော့ခလောက်တွေနဲ့ အစိမ်းရောင်အမှန်ခြစ်လေးက သူတို့ရဲ့ အတည်ပြုစစ်ဆေးမှု အောင်မြင်တာကို ရည်ညွှန်းပါတယ်။

အခြားစနစ်တစ်ခုခုကို သုံးပြီး စကားဝှက်သော့များကို အတည်ပြုခြင်း

အကယ်၍ လူချင်းတွေ့ဆုံပြီး စကားဝှက်သော့ကို အတည်ပြုဖို့မဖြစ်နိုင်ဘူးဆိုရင်တော့ စကားဝှက်သော့ကို သုံးမယ့် ဆက်သွယ်ရေးနည်းလမ်းမဟုတ်တဲ့ အခြားနည်းလမ်းတစ်ခုခုကို သုံးပြီး သင့်မိတ်ဆွေကို ဆက်သွယ်ဖို့လိုပါတယ်။

ဥပမာအားဖြင့် သင့်က PGP စကားဝှက်သော့ကို စစ်ဆေးအတည်ပြုမယ်ဆိုရင် ဖုန်း (သို့) OTR ချက်ကို သုံးလို့ရပါတယ်။ သင့်စကားဝှက်ကို အတည်ပြုမယ့်စနစ်ထက် ပိုပြီးလုံခြုံတဲ့ စနစ်ကို သုံးပြီး အတည်ပြုစစ်ဆေးပါ (ဥပမာ- ကုဒ်ဖြင့်ပြောင်းလဲခြင်းကို သုံးတဲ့ အခြားဆက်သွယ်ရေးစနစ်)။ ဘာလို့လဲဆိုတော့ အဲဒီလိုလုပ်ခြင်းအားဖြင့် သင့်မက်ဆေ့ချ်တွေကို ကြားဖြတ်ရယူဖို့ကြိုးစားတဲ့သူက စနစ်အကုန်လုံးကနေ တပြိုင်နက်တည်း လိမ်လည်လှည့်ဖျားဖို့ ခက်လို့ပါပဲ။

အန်မင်းနဲ့ ဂါဆန်းက PGP ကို သုံးကြမယ်ဆိုပါစို့။ အန်မန်းက Signal ကတဆင့် သူ့ရဲ့ PGP အများသုံး စကားဝှက်သော့ လက်ဗွေကို ဂါဆန်းဆီ ပို့လိုက်မယ်။ ဂါဆန်းက အန်မင်းပို့လိုက်တဲ့ လက်ဗွေကို သူ့ဆီမှာရှိတဲ့ အများသုံးစကားဝှက်သော့ဖိုင်နဲ့ တိုက်ဆိုင်စစ်ဆေးမယ်။

ဘယ်ဘက်က လက်ပ်တော့မှာ PGP အများသုံးသော့၊ ကိန်းဂဏန်း ၄လုံးပါ ကိန်းစဉ် ၁၀ ခုတွဲနဲ့ အပြိုးမျက်နှာတို့ကို တွေ့ရပါမယ်။ ညာဘက်က စမတ်ဖုန်းမှာတော့ အတည်ပြုမယ့်နည်းလမ်း ဖြစ်တဲ့ Signal အက်ပ်ကိုဖွင့်ထားပြီး တူညီတဲ့ အပြိုးမျက်နှာနဲ့ ကိန်းဂဏန်း ၄ လုံးပါ ကိန်းစဉ် ၁၀ ခုတွဲကို တွေ့ရပါမယ်။

ဘယ် အက်ပ်ကိုပဲသုံးသုံး သင့်အနေနဲ့ သင့်ရဲ့ သော့နဲ့ သင့်မိတ်ဆွေရဲ့သော့တွေရဲ့ တည်နေရာကို ရှာလို့ ရပါတယ်။

သော့တွေရဲ့တည်နေရာကို ရှာရတဲ့တည်းလမ်းက အမျိုးမျိုးရှိပေမဲ့ စကားဝှက်သော့ အတည်ပြုတဲ့ နည်းလမ်းတွေကတော့ ခပ်ဆင်ဆင်တူကြတာချည်းပါပဲ။ သင့်ရဲ့ စကားဝှက်သော့လက်ဗွေနံပါတ် တွေကို (မျက်နှာချင်းဆိုင်/ ဖုန်းကတဆင့်) နှုတ်တိုက်ရွတ်လို့ရသလို အခြားဆက်သွယ်ရေး နည်းလမ်းမှာ ကော်ပီ၊

ပေ့စ်လုပ်ပြီးပို့လို့ရပါတယ်။ အရေးကြီးတာက စကားလုံးနဲ့ နံပါတ်တစ်ခုချင်းစီကို တိုက်ဆိုင်စစ်ဆေးဖို့ပါပဲ။

အစ-အဆုံးကုဒ်ဖြင့် ပြောင်းလဲခြင်းစနစ်ကို

အစ-အဆုံးကုဒ်ဖြင့် ပြောင်းလဲခြင်းစနစ်ကို သုံးထားတဲ့ မက်ဆေ့ချ်ပေးပို့တဲ့ အက်ပ်အတော်များများမှာ စကားဝှက်သော့ပြောင်းသွားတာကို ဖော်ပြတဲ့စနစ်ပါရှိတတ်ပါတယ်။ အရှေ့မှာပြောခဲ့သလိုပဲ သင့်မိတ်ဆွေတစ်ဦးဦးရဲ့ စကားဝှက်သော့ပြောင်းသွားတာနဲ့ စစ်ဆေးအတည်ပြုတာကို မပျက်မကွက်လုပ်ဆောင်ဖို့ လိုပါတယ်။ လူချင်းတွေ့ပြီးတော့ပဲဖြစ်ဖြစ် အခြားလုံခြုံတဲ့စနစ်ကိုပဲ ဖြစ်ဖြစ် သုံးလို့ရပါတယ်။ ဥပမာ- အချို့တွေဆိုရင် သူတို့တွေဖုန်းလဲကိုင်တဲ့အခါ မလဲခင်မှာ မိတ်ဆွေတွေကို ကြိုတင်အသိပေး ထားလိုက်ရင် စကားဝှက်သော့ပြောင်းတဲ့အခါ သို့လောသို့လော မဖြစ်တော့ဘူးပေါ့။

သင့်မိတ်ဆွေတစ်ဦးဦးနဲ့ အတူစကားဝှက်သော့ကို စစ်ဆေးအတည်ပြုကြည့်ပါ။ ဘယ်အက်ပ်အတွက် ဘယ်လိုလုပ်ရမယ်ဆိုတာကို အက်ပ်ရဲ့ လမ်းညွှန်မှာ ဖတ်လို့ရပါတယ်။

PGP ၏ ယုံကြည်မှုကွန်ယက်နှင့် အခြားစကားဝှက်သော့အတည်ပြုခြင်း အထောက်အကူများ

သင့်မှာ ဆက်သွယ်အတည်ပြုရမယ့်သူတွေ အရမ်းများနေရင် စနစ်ပြင်ပ စကားဝှက်သော့ အတည်ပြုခြင်း နည်းလမ်းကို သုံးဖို့ခက်ပါလိမ့်မယ်။ အဲဒီနည်းလမ်းကို အသုံးမပြုနိုင်တဲ့အခါမှာ သင်ဟာ မှန်ကန်တဲ့ စကားဝှက်သော့ အသုံးပြုနေကြောင်း ဆန်းစစ်နိုင်တဲ့ နည်းလမ်းအချို့ ရှိပါသေးတယ်။

PGP က အခြားသူတွေရဲ့ စကားဝှက်သော့တွေမှာ သင့်လက်မှတ်ထိုးဖို့ လုပ်ဆောင်ပေးပါတယ်။ ဆိုလိုတာက သော့က တကယ်မှန်ကန်တဲ့သူဆီက ဖြစ်ကြောင်း သင့်အနေနဲ့အာမခံပေးလို့ရပါတယ်။ PGP အသုံးပြုသူတွေနေနဲ့ စကားဝှက်သော့လက်မှတ်ထိုးပွဲတွေမှာ ဆုံတွေ့လို့ရပါတယ်။ အဲဒီပွဲတွေမှာ တစ်ယောက်ကိုတစ်ယောက် မည်သူမည်ဝါဖြစ်ကြောင်း အတည်ပြုပြီး စကားဝှက်သော့တွေမှာ လက်မှတ်ထိုးလို့ရပါတယ်။ သင့်ရဲ့ PGP ဆော့ဖ်ဝဲလ်က စကားဝှက်သော့တစ်ခုမှာ ထိုးထားတဲ့ လက်မှတ်အရေအတွက်ကိုကြည့်ပြီး ယုံသင့်၊ မယုံသင့်ကို ဆုံးဖြတ်ပေးပါလိမ့်မယ်။ PGP အသုံးပြုသူကွန်ယက်ထဲမှာ အချင်းချင်းအာမခံပေးတာမို့ “ယုံကြည်မှုကွန်ယက်” လို့လည်း ခေါ်ကြပါတယ်။ ဒါပေမဲ့ လူကိုယ်တိုင်တွေ့ပြီး စစ်ဆေးအတည်ပြုတာလောက်တော့ မသေချာဘူးပေါ့။

“ယုံကြည်မှုကွန်ယက်” ကြောင့် PGP မှာ သင့်ရဲ့ မိတ်ဆွေသစ်တွေရဲ့ စကားဝှက်သော့တွေကို လည်း PGP စကားဝှက်သော့ဆာဗာတွေကနေ ဒေါင်းလုတ်ဆွဲလို့ ရပါတယ်။ သင့်ဆော့ဖ်ဝဲလ်က သင့်ရဲ့ အီးမေးလ်နဲ့ စကားဝှက်သော့ကို တွဲပြီး စကားဝှက်သော့ဆာဗာဆီထဲကို upload လုပ်လို့ရပါတယ်။ PGP

အသုံးပြုသူက အီးမေးလ်တစ်ခုအတွက် မှန်ကန်တဲ့ စကားဝှက်သော့ကို PGP စကားဝှက်သော့ ဆာဗာကနေ ရယူနိုင်ပါတယ်။

ဒါပေမဲ့ အီးမေးလ်ပစ်စာတစ်ခု (သို့မဟုတ်) လူတစ်ယောက် ဟန်ဆောင်ပြီး စကားဝှက်သော့အများတွေ upload လုပ်တာကိုတော့ တားနိုင်တဲ့နည်းလမ်းမရှိသေးပါဘူး။ ဒါမျိုးတွေလည်း ဖြစ်ခဲ့ဘူးပါတယ်။ ဒါပေမယ့် သင်သိတဲ့သူတွေ အတော်များများက လက်မှတ်ထိုးထားတယ်ဆိုရင်တော့ အဲဒီသော့က အစစ်ဖြစ်ဖို့ များပါတယ်။ ဖြစ်နိုင်ရင်တော့ လူချင်းတွေ့ပြီး အတည်ပြုတာလောက် ဘယ်အရာမှ စိတ်မချရပါဘူး။

အယောင်ဆောင်ထားတဲ့ လူတစ်ယောက်က မူလစကားဝှက်သော့ရဲ့ လက်ဗွေနဲ့ဆင်တူတဲ့ စကားဝှက်သော့ကို ဆွဲတင်ထား နိုင်ပါသေးတယ်။ ဒါ့ကြောင့်မို့ စာလုံးတိုင်း၊ ကိန်းဂဏန်းတိုင်းကို တစ်လုံးမကျန် တိုက်ဆိုင်စစ်ဆေးဖို့ အထူးသတိပြုပါ။

Keybase လိုမျိုး အချို့ဝန်ဆောင်မှုတွေမှာဆိုရင် သော့ပိုင်ရှင် စစ်မှန်ကြောင်းကို ဆိုရှယ်မီဒီယာက တဆင့် အတည်ပြုတာမျိုး ရှိပါတယ်။ ဒီဝန်ဆောင်မှုတွေမှာဆိုရင် စကားဝှက်သော့တစ်ခုကို အသုံးပြုသူဟာ တွစ်တာအကောင့် (သို့) ဖေ့ဘုတ်အကောင့်ကသူနဲ့ တစ်ဦးတည်းဖြစ်ကြောင်းကို တိုက်ဆိုင်စစ်ဆေးပေးပါတယ်။ ဒီလိုလုပ်တာကလည်း သော့နဲ့ သော့ပိုင်ရှင်မှန်ကန်ကြောင်း သက်သေခံလို့ရပေမဲ့ လူချင်းတွေ့တာလောက်တော့ စိတ်မချရပါဘူး။

အများသုံးစကားဝှက်သော့တွေနဲ့ စကားဝှက်သော့ စစ်ဆေးအတည်ပြုခြင်းနဲ့ ပတ်သက်လို့ ပိုပြီး သိချင်တယ်ဆိုရင် Surveillance Self-Defense လမ်းညွှန်တွေဖြစ်တဲ့ ကုဒ်ဖြင့်ပြောင်းလဲခြင်း၏ အဓိက အယူအဆများ နဲ့ အစ-အဆုံးကုဒ်ဖြင့် ပြောင်းလဲခြင်းအား နက်နဲစွာလေ့လာခြင်းတို့ကို ဖတ်ရှုလေ့လာနိုင်ပါတယ်။