EFF'S SURVEILLANCE SELF-DEFENSE

ကုန်ဖြင့်ပြောင်းလဲခြင်းနဲ့ပတ်သက်လို့ ဘာတွေသိထားသင့်သလဲ။

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

LOCALIZATION LAB

ကုဒ်ဖြင့်ပြောင်းလဲခြင်းနဲ့ပတ်သက်လို့ ဘာတွေသိထားသင့်သလဲ။

နောက်ဆုံးစိစစ်သည့်ရက်စွဲ - ၂၀၂၁ ခုနှစ် ဇွန်လ ၃ ရက်

“ကုဒ်ဖြင့်ပြောင်းလဲခြင်း encryption” ဆိုတဲ့ ဝေါဟာရနဲ့ပတ်သက်ပြီး နေရာအမျိုးမျိုးမှာ ပုံစံအမျိုးမျိုးနဲ့ကြားဖူးပါလိမ့်မယ်။ တကယ်တော့ **ကုဒ်ဖြင့်ပြောင်းလဲခြင်း** ဆိုတာ မက်ဆေ့ချ်တစ်ခုကို တခြားမဆိုင်သူတွေ ဖတ်မရဘဲ ဝှက်စာဖြစ်သွားအောင် ကုဒ်နဲ့ပြောင်းတဲ့ သင်္ချာနည်းပညာပါ။ ကုဒ်ကို ပြန်ဖြည် “decrypt” နိုင်တဲ့ သော့ key ရှိသူသာ အဲဒီမက်ဆေ့ချ်ကို ဖတ်လို့ရပါတယ်။

သမိုင်းတလျှောက်မှာ လူတွေဟာ မိမိပို့တဲ့ မက်ဆေ့ချ်တွေကို ရည်ရွယ်သူကလွဲလို့ အခြားသူတွေ ကြားဖြတ်ဖတ်မရစေဖို့ ကုဒ်အမျိုးမျိုးသုံးပြီး ဝှက်စာရေးနည်းတွေကို အသုံးပြုခဲ့ပါတယ်။ အခုခေတ်မှာတော့ ဝှက်စာရေးဖို့အတွက် ကွန်ပျူတာတွေကို အသုံးပြုနိုင်ပါပြီ။ ဒီဂျစ်တယ်နည်းပညာသုံး ကုဒ်ဖြင့်ပြောင်းလဲခြင်း နည်းပညာက ရိုးရှင်းတဲ့လျှို့ဝှက်မက်ဆေ့ချ်ပို့တာထက်ပိုပြီး လုပ်ဆောင်နေနိုင်ပါပြီ။ နမူနာဆိုရရင် မက်ဆေ့ချ်တွေကို ရေးပို့သူကို အတည်ပြုတာမျိုးပေါ့။

ကုဒ်ဖြင့်ပြောင်းလဲခြင်းဆိုတာ ကိုယ့်ရဲ့အချက်အလက်တွေကို မကောင်းတဲ့သူတွေ၊ အစိုးရတွေနဲ့ ဝန်ဆောင်မှုပေးသူတွေရန်က ကာကွယ်ဖို့အတွက် အကောင်းဆုံးသော နည်းပညာလို့ဆိုနိုင်ပါတယ်။ ပြီးတော့ သေသေချာချာစေ့စေ့စပ်စပ်အသုံးပြုမယ်ဆိုရင် သော့မရှိသူဘယ်သူမှ ပြန်ဖြည်လို့မရအောင် လုပ်နိုင်တဲ့အထိ နည်းပညာကတိုးတက်နေပါပြီ။

ဒီလမ်းညွှန်မှာ ကုဒ်ဖြင့်ပြောင်းလဲခြင်း နည်းလမ်း (၂) မျိုးဖြစ်တဲ့ အထိုင်ဒေတာကို ကုဒ်ဖြင့်ပြောင်းလဲခြင်းနဲ့ ရွေ့လျားဒေတာကို ကုဒ်ဖြင့်ပြောင်းလဲခြင်း အကြောင်းတွေကို တင်ပြပေးသွားပါမယ်။

အထိုင်ဒေတာကို ကုဒ်ဖြင့်ပြောင်းလဲခြင်း

“အထိုင်ဒေတာ (data at rest)” ဆိုတာ တနေရာရာမှာသိမ်းထားတဲ့ ဒေတာတွေကို ဆိုလိုပါတယ်။ ဥပမာ- မိုဘိုင်းဖုန်း၊ လက်ပ်တော့၊ ဆာဗာ (သို့မဟုတ်) ဟာ့ဒ်ရိုက်။ အထိုင်ဒေတာဆိုတာ တနေရာကနေ တနေရာသို့ရွေ့လျားခြင်းမရှိဘဲ ပုံသေနေရာတစ်ခုမှာရှိနေတဲ့ ဒေတာလို့လည်း နားလည်နိုင်ပါတယ်။

အထိုင်ဒေတာကို ကုဒ်ဖြင့်ပြောင်းလဲခြင်းအတွက် အသုံးပြုတဲ့နည်းလမ်းတစ်ခုကို ဥပမာပေးရမယ်ဆို ရင် “အပြည့်အဝကုဒ်ဖြင့်ပြောင်းလဲခြင်းစနစ် (သို့) စက်ပစ္စည်းကို ကုဒ်ဖြင့်ပြောင်းလဲခြင်း (full-disk encryption (သို့) device encryption) အကြောင်းပြောပြပါမယ်။ အပြည့်အဝကုဒ်ဖြင့်ပြောင်းလဲခြင်း စနစ်ဆိုတာ ဝှက်စာကြောင်း passphrase နည်းလမ်း (သို့မဟုတ်) အခြားအတည်ပြုသက်သေခံခြင်း နည်းလမ်းတစ်မျိုးမျိုးကို သုံးပြီး စက်ပစ္စည်းတစ်ခုအတွင်းမှာ သိုလှောင်ထားတဲ့ အချက်အလက်တွေ အားလုံးကို အကာအကွယ်အပေးထားတာပါ။ မိုဘိုင်းစက်ပစ္စည်း (သို့မဟုတ်) လက်ပ်တော့ တစ်ခုမှာပါတဲ့ စက်ပစ္စည်းကို လော့ခ်ချတဲ့စခရင်လိုပါပဲ၊ စကားဝှက်တစ်ခု၊ ဝှက်စာကြောင်းတစ်ခု၊ လက်ဗွေနဲ့ ဖွင့်ရတာပါ။ ဒါပေမဲ့သင့်စက်ပစ္စည်းကို စကားဝှက် password သုံးပြီး လော့ခ်ချထားရုံနဲ့ အဲဒီစက်မှာ အပြည့်အဝကုဒ်ဖြင့်ပြောင်းလဲခြင်းစနစ်ကို ဖွင့်ထားတယ်လို့ မှတ်ယူလို့မရပါဘူး။

စမတ်ဖုန်းနဲ့ လက်ပ်တော့တွေမှာ စကားဝှက်နဲ့ သော့ခတ်လို့ရတဲ့ လော့ခ်စခရင် ပါပါတယ်။

သင့်ရဲ့ကွန်ပျူတာလည်ပတ်မှုစနစ် operating system မှာ အပြည့်အဝကုဒ်ဖြင့်ပြောင်းလဲခြင်း စနစ်ကို ဖွင့်ထားလားဆိုတာကို စစ်ဆေးဖို့မမေ့ပါနဲ့။ အချို့ ကွန်ပျူတာလည်ပတ်မှုစနစ်တွေမှာ အပြည့်အဝကုဒ်ဖြင့်ပြောင်းလဲခြင်းစနစ်ကို အလိုအလျောက်ဖွင့်ပေးထားပါတယ်။ အချို့ကတော့ အဲဒီလိုမဟုတ်ပါဘူး။ ဆိုလိုတာက ကုဒ်ဖြင့်ပြောင်းလဲခြင်းအတွက် ပြန်ဖြည်တဲ့သော့မလိုဘဲ သင့်စက်ပစ္စည်းရဲ့ လော့ခ်ကို ဖွင့်လိုက်နိုင်တာနဲ့ ဒေတာတွေအကုန် ရသွားနိုင်ပါတယ်။ အချို့စနစ်တွေမှာတော့ အပြည့်အဝကုဒ်ဖြင့် ပြောင်းလဲခြင်းစနစ်ကို ဖွင့်ထားရင်တောင် RAM (ကျပန်းကွန်ပျူတာ မှတ်ဉာဏ်စနစ်) မှာ ကုဒ်နဲ့ပြောင်းလဲမထားတဲ့ စာတွေကို ဒီအတိုင်း သိမ်းထား တာမျိုးလည်းရှိတတ်ပါ

တယ်။ RAM ဆိုတာ ဒေတာတွေကို ခေတ္တသိုလှောင်တဲ့နေရာဖြစ်ပြီး သင့်စက်ပစ္စည်းကို ပါဝါပိတ်လိုက်တာနဲ့ သိမ်းထားတာတွေကို ဖတ်လို့မရတတ်တော့ပါဘူး။ ဒါပေမဲ့ လက်စောင်းထက်တဲ့ တိုက်ခိုက်သူတွေက cold boot attack လိုမျိုးနဲ့တိုက်ခိုက်မယ်ဆိုရင်တော့ RAM ထဲမှာရှိတဲ့ ဒေတာတွေကို ရယူသွားနိုင်ပါတယ်။

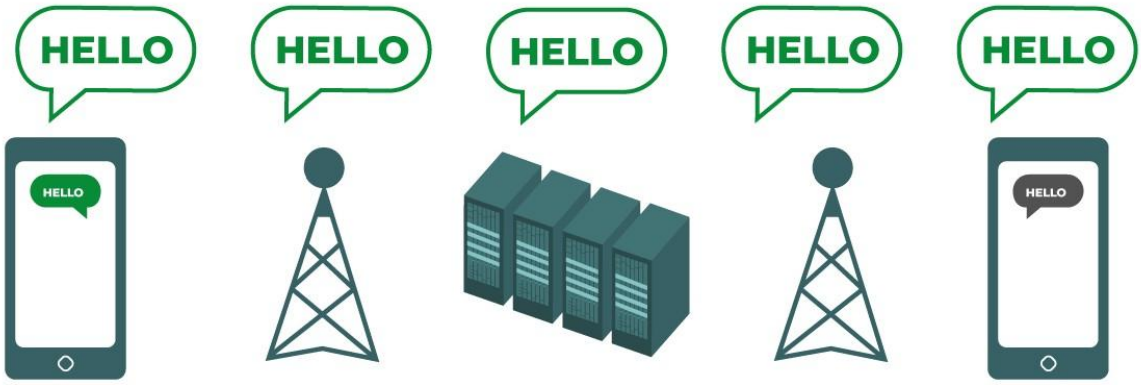
အပြည့်အဝကုဒ်ဖြင့်ပြောင်းလဲခြင်းစနစ်က သင့်စက်ပစ္စည်းကို ကိုင်တွယ်လို့ရတဲ့ အနီးအနားက သူတွေရဲ့ ရန်ကနေ ကာကွယ်ပေးနိုင်ပါတယ်။ သင့်ရဲ့အခန်းဖော်တွေ၊ လုပ်ဖော်ကိုင်ဖက်တွေ၊ ဝန်ထမ်းတွေ၊ ကျောင်းတာဝန်ခံတွေ၊ မိသားစုဝင်တွေ၊ အပေါင်းအဖော်တွေ၊ ရဲဝန်ထမ်းတွေနဲ့ အခြား ဥပဒေဆိုင်ရာဝန်ထမ်းတွေရဲ့ ရန်ကနေ သင့်ဒေတာတွေကို ကာကွယ်ဖို့သုံးနိုင်ပါတယ်။ ဒါ့အပြင် သင့်စက်ပစ္စည်းတွေ အခိုးခံရတာမျိုး၊ ပျောက်ရှတာမျိုး (ဥပမာ- စားသောက်ဆိုင် (သို့) ဘတ်စ်ကားပေါ်မှာ မတော်တဆမေ့ကျန်ခဲ့တာ) ဖြစ်ခဲ့ရင်တောင်မှ ကုဒ်ဖြင့်ပြောင်းလဲခြင်းနည်းပညာက သင့်ဒေတာတွေကို အကာအကွယ်ပေးနိုင်ပါလိမ့်မယ်။

အထိုင်ဒေတာတွေကို ကုဒ်နဲ့ပြောင်းလဲခြင်း encrypt အတွက် အခြားနည်းလမ်းတွေ ရှိပါသေးတယ်။ အဲ့ဒီနည်းလမ်းတွေထဲကတစ်ခုကတော့ ကွန်ပျူတာ (သို့) ဒေတာတွေသိမ်းထားတဲ့ စက်ပစ္စည်းတမျိုးမျိုးထဲက ဖိုင်တစ်ခုချင်းစီကို ကုဒ်ဖြင့်ပြောင်းရေးနိုင်တဲ့ “ဖိုင်ကိုကုဒ်ဖြင့်ပြောင်းလဲခြင်း (file encryption)” နည်းလမ်းဖြစ်ပါတယ်။ နောက်ထပ်နည်းလမ်းကတော့ “ဒရိုက်ကိုကုဒ်ဖြင့်ပြောင်းလဲခြင်း” (ဒစ်ခ်ကိုကုဒ်ဖြင့်ပြောင်းလဲခြင်းဟုလည်းခေါ်တွင်) (drive encryption/ disk encryption) နည်းလမ်း ဖြစ်ပြီး စက်ပစ္စည်းထဲက ဒေတာသိမ်းထားတဲ့နေရာတွေထဲကမှ မိမိလိုချင်တဲ့ နေရာကို ရွေးချယ်သတ် မှတ်ပြီး ကုဒ်ဖြင့်ပြောင်းလဲတဲ့နည်းလမ်းဖြစ်ပါတယ်။

ဒီနည်းလမ်းတွေကို မိမိစိတ်ကြိုက်တွဲပြီး သုံးလို့ရပါတယ်။ ဥပမာ- သင့်ရဲ့ ဆေးမှတ်တမ်းတွေကို လုံလုံခြုံခြုံသိမ်းဆည်းချင်တယ်ဆိုပါစို့။ သင့်အနေနဲ့ စက်ထဲမှာသိမ်းထားတဲ့ ဆေးမှတ်တမ်းဖိုင်တစ်ခုတည်းကို **ဖိုင်ကိုကုဒ် ဖြင့်ပြောင်းလဲခြင်း** နည်းလမ်းနဲ့ ပြောင်းလို့ရပါတယ်။ ဒါ့အပြင် **ဒရိုက်ကိုကုဒ်ဖြင့်ပြောင်းလဲခြင်း** နည်းလမ်းကို သုံးပြီး သင့်ဆေးမှတ်တမ်းသိမ်းထားတဲ့နေရာကို ကုဒ်နဲ့ပြောင်းလဲလို့ရပါတယ်။ ထပ်ပြီး **အပြည့်အဝကုဒ်ဖြင့်ပြောင်းလဲခြင်း** နည်းလမ်းကိုသုံးပြီး ဆေးမှတ်တမ်းဖိုင်အပြင် စက်တစ်ခုလုံးထဲမှာ သိမ်းထားတဲ့ ကွန်ပျူတာ လည်ပတ်မှုစနစ်ဖိုင်တွေအပါအဝင် ဖိုင်တွေအားလုံးကိုကုဒ်နဲ့ပြောင်းလဲလိုက်လို့ရပါတယ်။

“စောင့်ကြည်ထောက်လှမ်းမှုအတွက်ကိုယ်ပိုင်ခုခံကာကွယ်ခြင်း (SSD)” မှာ သင့်စက်ပစ္စည်းတွေကို ကုဒ်ဖြင့်ပြောင်းလဲခြင်းလုပ်နိုင်မယ့် နည်းလမ်းလမ်းညွှန်ချက်အချို့ guides for enabling encryption ကို ရေးသားဖော်ပြပြီးဖြစ်ပါတယ်။ အခြားကုဒ်ဖြင့်ပြောင်းလဲခြင်း နည်းလမ်းတွေအကြောင်းကို ထဲထဲဝင်ဝင်ထပ်သိချင်တယ်ဆိုရင်တော့ အွန်လိုင်းနဲ့ SSD ဆိုက်မှာဆက်ရှာကြည့်လို့ရပါတယ်။ တစ်ခုသတိပြုရမှာက လုပ်ဆောင်နိုင်တဲ့နည်းလမ်းတွေက အပြောင်းအလဲရှိနိုင်ပြီး ဒီလမ်းညွှန်တွေကလည်း ခေတ်နဲ့မညီတော့တာမျိုးလည်း အချိန်မရွေး ဖြစ်နိုင်တယ်ဆိုတာပါ။

ရွှေ့လျားဒေတာကို ကုဒ်ဖြင့်ပြောင်းလဲခြင်း



ဒီပုံကားချပ်က ကုဒ်နဲ့ပြောင်းလဲမထားတဲ့ဒေတာကို နေရာတစ်ခုကနေ အခြားနေရာတစ်ခုကို ပို့နေတဲ့ ပုံကိုပြတာပါ။ ဒီပုံက အင်တာနက်ဝန်ဆောင်မှုပေးတဲ့နေရာတွေမှာ မူလဖြစ်နေတဲ့ပုံစံပါ။ ဘယ်ဘက်မှာ စမတ်ဖုန်းတစ်လုံးကနေ ကုဒ်နဲ့ပြောင်းလဲမထားတဲ့ အစိမ်းရောင်နဲ့ရေးထားတဲ့ မက်ဆေ့ချ်ကို ညာဘက်မှာရှိတဲ့ စမတ်ဖုန်းဆီကို ပို့နေပါတယ်။ ပို့တဲ့လမ်းတလျှောက်မှာဆိုရင် မက်ဆေ့ချ်က တာဝါတိုင်တစ်ခုကနေ ကုမ္ပဏီဆာဗာတွေထဲဝင်တယ်။ ပြီးတာနဲ့ အခြားတာဝါတစ်ခုဆီကို ကုဒ်နဲ့ပြောင်းလဲထားခြင်း မရှိတဲ့ "ဟဲလို" ဆိုတဲ့ စာတိုကိုပို့ပေးပါတယ်။ မက်ဆေ့ချ်ဖြတ်သွားတဲ့ ကွန်ပျူတာနဲ့ နက်ဝေါ့ခ်တွေအားလုံးမှာ ဟဲလို ဆိုပြီး မြင်ရမှာဖြစ်သလို နောက်ဆုံးလက်ခံတဲ့ စမတ်ဖုန်းမှာလည်း ဟဲလို လို့မြင်ရမှာဖြစ်ပါတယ်။

"ရွှေ့လျားဒေတာ" ဆိုတာက နက်ဝေါ့ခ်တလျှောက် တနေရာကနေတနေရာကို ရွှေ့လျားစီးဆင်းနေတဲ့ သတင်းအချက်အလက်တွေဖြစ်ပါတယ်။ နမူနာဆိုရရင် သင်ကမက်ဆေ့ချ်အက်ပ်တစ်ခုကို သုံးပြီး မက်ဆေ့ချ်ပို့တဲ့အခါ အဲဒီမက်ဆေ့ချ်က သင့်စက်ပစ္စည်းကနေတဆင့် အက်ပ်ကုမ္ပဏီရဲ့ဆာဗာတွေကို ဖြတ်ပြီး သင့်ပို့လိုက်တဲ့သူရဲ့စက်ပစ္စည်းထဲဖြတ်စီးရတာမျိုးပေါ့။ နောက်ထပ် နမူနာတစ်ခုကတော့ ဘရာက်ဇာသုံးပြီး ဝက်ဘ်ဆိုက်ထဲဝင်ကြည့်တဲ့အခါ ဝက်ပေ့ချ်တစ်ခုမှာရှိတဲ့ ဒေတာတွေက ဝက်ဘ်ဆိုက်ဆာဗာတွေက တဆင့် သင့်ဘရောက်ဇာထဲ ဖြတ်သန်းစီးဝင်လာရတာမျိုးပါ။

အချို့နာမည်ကြီးအက်ပ်တွေမှာ မက်ဆေ့ချ်တွေရဲ့လုံခြုံမှုအတွက် ဝန်ဆောင်မှုတွေပါတတ်ပါတယ်။ ဥပမာ - မက်ဆေ့ချ်တွေကိုဖတ်ပြီးတာနဲ့ ပျောက်သွားအောင်လုပ်တာမျိုးပေါ့။ ဒီနေရာမှာ လုံခြုံစိတ်ချရတယ်လို့ခံစားရစေတဲ့ ဆက်သွယ်ရေးနည်းလမ်းတိုင်း (ချက်/ မက်ဆေ့ချ်ပို့ခြင်း) က စစ်မှန်တဲ့လုံခြုံမှုကို မပေးနိုင်ဘူးဆိုတာကို သတိပြုရပါမယ်။ သင့်မက်ဆေ့ချ်ဖြတ်သန်းစီးဆင်းသွားတဲ့ ကွန်ပျူတာတိုင်းမှာ အဲဒီမက်ဆေ့ချ်ကို ဖတ်လို့ရနေတာမျိုးဖြစ်နိုင်ပါတယ်။

သင်နဲ့ သင်ချိတ်ဆက်တဲ့သူအကြားက ဆက်သွယ်မှုတွေအားလုံး လုံခြုံမှုရှိစေဖို့ ကုဒ်နဲ့ ပြောင်းလဲထားတယ်ဆိုတာကို အတည်ပြုထားဖို့လိုတဲ့အပြင် “သယ်ယူပို့ဆောင်ရေးအလွှာတွင်ကုဒ်ဖြင့်ပြောင်းလဲခြင်း” transport-layer encryption နဲ့ “အစ - အဆုံးကုဒ်ဖြင့်ပြောင်းလဲခြင်း” end-to-end encryption ဆိုတဲ့ နည်းလမ်း နှစ်မျိုးထဲက ဘယ်နည်းလမ်းကတဆင့် ပြောင်းလဲထားတယ်ဆိုတာကို ဆိုတာကို သိထားဖို့လိုပါတယ်။

ရွှေ့လျားဒေတာတွေအတွက် ကုဒ်ဖြင့်ပြောင်းလဲခြင်းအတွက် နည်းလမ်းနှစ်မျိုးရှိပါတယ်။ **သယ်ယူပို့ဆောင်ရေး အလွှာတွင်ကုဒ်ဖြင့်ပြောင်းလဲခြင်း** နဲ့ **အစ - အဆုံးကုဒ်ဖြင့်ပြောင်းလဲခြင်း** တို့ဖြစ်ပါ တယ်။ ဘယ်ဝန်ဆောင်မှုက ဘယ်နည်းလမ်းကိုအသုံးပြုတယ်ဆိုတာသိမှ ဘယ်အက်ပ်က ကိုယ်နဲ့သင့်တော်သလဲဆိုတာ ဆုံးဖြတ်လို့ရမှာပါ။ အောက်မှာပြထားတဲ့ ဥပမာတွေကိုကြည့်ပြီး နည်းလမ်း (၂) မျိုး ရဲ့ ကွာခြားချက်ကို လေ့လာနိုင်ပါတယ်။

သယ်ယူပို့ဆောင်ရေး အလွှာတွင်ကုဒ်ဖြင့်ပြောင်းလဲခြင်း

ဒီပုံကားချပ်ကတော့ သယ်ယူ ပို့ဆောင်ရေးအလွှာတွင်ကုဒ်ဖြင့်ပြောင်းလဲခြင်းကို သရုပ်ဖော်ထားတာဖြစ်ပါတယ်။ ဘယ်ဘက်က စမတ်ဖုန်းကနေ “ဟဲလို” ဆိုတဲ့ ကုဒ်ဖြင့်ပြောင်းလဲထားခြင်း မရှိတဲ့ အစိမ်းရောင်မက်ဆေ့ချ်ကို ပို့လိုက်ပါတယ်။ အဲဒီမက်ဆေ့ချ်ကို ကုဒ်နဲ့ပြောင်းလဲပြီး ဖုန်းတာဝါတိုင်ဆီ ထပ်ပို့လိုက်ပါတယ်။ ဒီလိုပို့နေစဉ်မှာ ကုမ္ပဏီဆာဗာတွေဆီရောက်ရင် မက်ဆေ့ချ်ကို ကုဒ်နဲ့ပြောင်းလဲတာကိုပြန်ဖြည် decrypt မယ်၊ ပြီးတာနဲ့ ပြန်ပြီးကုဒ်နဲ့ပြောင်းလဲခြင်းကို ထပ်လုပ်ပေးပြီး နောက်ဖုန်းတာဝါတိုင်တစ်ခုဆီ မက်ဆေ့ချ်ကိုပို့ပေးမယ်။ နောက်ဆုံးမှာတော့ လက်ခံရရှိသူက ကုဒ်နဲ့ပြောင်းလဲထားတဲ့မက်ဆေ့ချ်ကိုရမယ်။ အဲဒါကိုပြန်ဖြည်လိုက်တဲ့ အခါမှာတော့ “ဟဲလို” လို့ဖတ်လို့ရပြီပေါ့။

သယ်ယူ ပို့ဆောင်ရေး အလွှာတွင်ကုဒ်ဖြင့်ပြောင်းလဲခြင်းကို သယ်ယူ ပို့ဆောင်ရေး အလွှာလုံခြုံရေး transport layer security (TLS) လို့လဲခေါ်ဆိုကြပါတယ်။ ဘာလို့လဲဆိုတော့ သင်ပို့လိုက်တဲ့ မက်ဆေ့ချ်ကို သင့်စက်ပစ္စည်းကနေ အက်ပ်ဆာဗာဆီသယ်ယူပို့ဆောင်ချိန်နဲ့ အက်ပ်ဆာဗာကနေ လက်ခံရရှိသူရဲ့စက်ပစ္စည်းဆီ သယ်ယူပို့ဆောင်နေစဉ်မှာ လုံခြုံအောင်လုပ်ဆောင်ပေးလို့ပါပဲ။ တစ်ခုရှိတာက အက်ပ်ဝန်ဆောင်မှု (သို့မဟုတ်) သင့်ကြည့်နေတဲ့ ဝက်ဘ်ဆိုက်ရဲ့ ဆာဗာဆီမက်ဆေ့ချ်ရောက်ချိန်မှာတော့ ပြန်ဖြည်ထားတဲ့ မက်ဆေ့ချ်တွေကို မြင်ရမှာဖြစ်ပါတယ်။ ဆိုလိုတာက သင့်မက်ဆေ့ချ်တွေကို ကုမ္ပဏီဆာဗာမှာမြင်ရ (တခါတလေ ကုမ္ပဏီဆာဗာထဲသိမ်းထား) မှာ ဖြစ်တဲ့အတွက် သင့်လုံခြုံရေးအတွက် စိုးရိမ်စရာရှိပါတယ်။ ဥပဒေစိုးမိုးရေးဆိုင်ရာအဖွဲ့အစည်းတွေရဲ့

ညွှန်ကြားချက်အရ၊ ဒါမှမဟုတ် ကုမ္ပဏီဆာဗာတွေ ရဲ့ လုံခြုံရေးကျိုးပေါက်သွားချိန်တွေမှာ သင့်လုံခြုံရေးကိုထိခိုက်နိုင်ခြေများပါတယ်။

သယ်ယူပို့ဆောင်ရေး အလွှာတွင်ကုဒ်ဖြင့်ပြောင်းလဲခြင်းဥပမာ- HTTPS

ဒီပုံမှာ ဝက်ဘ်ဆိုက်လိပ်စာအကွက်ထဲရေးထားတဲ့ ssd.eff.org ဘေးမှာ “https://” နဲ့ အစိမ်းရောင်သော့လေးကို တွေ့ပါသလား။ HTTPS ဆိုတာ ကွန်ပ်တို့ဝက်ဘ်ပေါ်မှာ မကြာခဏကြုံရတဲ့ သယ်ယူပို့ဆောင်ရေးအလွှာတွင်ကုဒ်ဖြင့်ပြောင်းလဲခြင်းအတွက် နမူနာနည်းလမ်းတစ်ခုဖြစ်ပါတယ်။ အဲဒါက ကုဒ်နဲ့ပြောင်းလဲထားခြင်းမရှိတဲ့ HTTPထက် ပိုပြီးတော့ လုံခြုံပါတယ်။ ဘာ့ကြောင့်ပါလဲ။ အဖြေကတော့ သင်ဝင်ရောက်ကြည့်ရှုတဲ့ HTTPS ဝက်ဘ်ဆိုက်တွေရဲ့ဆာဗာတွေမှာ သင်ထည့်သွင်းလိုက်တဲ့ အချက်အလက်တွေ (ဥပမာ- မက်ဆေ့ချ်တွေ၊ ရှာဖွေမှုတွေ၊ အကြွေးဝယ်ကဒ်နံပါတ်တွေနဲ့ အကောင့်အချက်အလက်တွေ) ကို မြင်ရပေမဲ့ နက်ဝေါ့ခ်ထဲမှာ ကြားဖြတ်ကြည့်ရှုသူတွေအတွက်တော့ အဲဒီအချက်အလက်တွေကို ဖတ်လို့ရတဲ့ပုံစံနဲ့ မြင်ရမှာမဟုတ်လို့ပါပဲ။

တစုံတစ်ယောက်က နက်ဝေါ့ခ်ထဲမှာ ဘယ်ဝက်ဘ်ဆိုက်တွေကို သုံးစွဲသူတွေက ဝင်ရောက်ကြည့်ရှုနေလဲဆိုတာကို ထောက်လှမ်းကြည့်ရှုနေတယ်ဆိုရင် HTTP ချိတ်ဆက်မှုက ကာကွယ်ပေးနိုင်မှာ မဟုတ်ပါဘူး။ ဒါပေမဲ့ HTTPS ချိတ်ဆက်မှုကျတော့ သင့်အနေနဲ့ ဝက်ဘ်ဆိုက်တစ်ခုကိုသွားရင် ဘယ်ပေ့ခ်ျကို ဝင်ရောက်ကြည့်ရှုလဲဆိုတာကို ဖုံးကွယ်ပေးထားပါတယ်။ ကိုယ်ဝင်ရောက်ကြည့်ရှုတဲ့ ဆိုက်အမည်ရဲ့ မျဉ်းစောင်းအနောက်ကို ဆက်မြင်ရမှာမဟုတ်ပါဘူး။ ဥပမာ - သင်က HTTPS ချိတ်ဆက်မှုနဲ့ “https://ssd.eff.org/en/module/what-encryption” ကို ဝင်ရောက်ကြည့်ရှုတဲ့အခါ ကြားဖြတ်စောင့်ကြည့်သူကတော့ “https://ssd.eff.org” လို့ မြင်ရမှာဖြစ်ပါတယ်။

ဝက်ဘ်ပေါ်မှာချိတ်ဆက်မှုတွေအားလုံးကို HTTPS အဖြစ်ပြောင်းလဲဖို့ လုပ်နေတာ အတော်ခရီးရောက်နေပါပြီ။ HTTP မှာ လုံခြုံရေးနဲ့ ပတ်သက်လို့ ဘာမှမပါပေမဲ့ HTTPS ကတော့ သူ့နဂိုအတိုင်းမှာတင် လုံခြုံရေးစနစ်ပါလာပြီးသားဖြစ်လို့ပါပဲ။ HTTP နဲ့ တွဲထားတဲ့ ဝက်ဘ်ပေ့ခ်ျတွေအားလုံးက လုံခြုံမှုမရှိလို့ ကြားဖြတ်စောင့်ကြည့်တာတွေ၊ အကြောင်းအရာတွေ ခိုးထည့်တာ၊ cookie ခိုးတာ၊ login နဲ့ စကားဝှက် password ခိုးယူတာ၊ ဆင်ဆာဖြတ်တာနဲ့ အခြားပြဿနာပေါင်းစုံကြုံတွေ့နိုင်ပါတယ်။

HTTPS လုံခြုံမှုအမြင့်ဆုံးရဖို့ EFF's browser extension ဖြစ်တဲ့ HTTPS Everywhere ကို နေရာတိုင်းမှာ အသုံးပြုဖို့အတွက် အကြံပြုလိုပါတယ်။ ဝက်ဘ်ဆိုက်တစ်ခုမှာ HTTPS ရော၊ HTTP ရောနဲ့ ချိတ်ဆက်လို့ရရင် HTTPS Everywhere က HTTPS နဲ့ပဲ ချိတ်ဆက်အောင် အမြဲလုပ်ပေးထားမှာပါ။

တစ်ခုသတိပြုရမှာက HTTPS ဝန်ဆောင်မှုသုံးတိုင်းတော့ ဝက်ဘက်ဆိုက်က သုံးစွဲသူတွေရဲ့ ကိုယ်ရေးလုံခြုံမှုကို အာမခံပေးနိုင်ပါဘူး။ ဥပမာအားဖြင့် HTTPS နဲ့ ကာကွယ်ထားတဲ့ဆိုက်တွေမှာ ခြေရာခံ cookies ဒါမှမဟုတ် အထိုင် (host) malware တွေကို သုံးနိုင်ပါသေးတယ်။

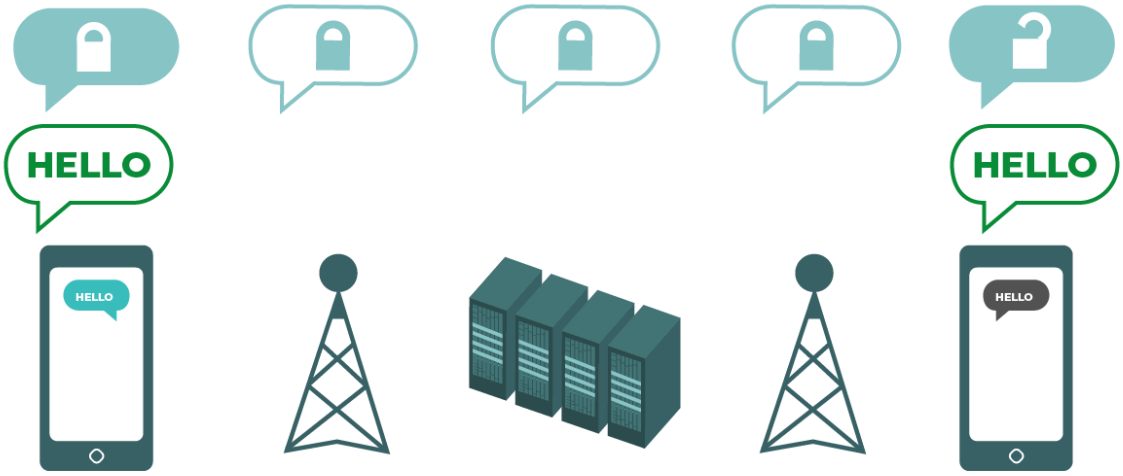
သယ်ယူပို့ဆောင်ရေး အလွှာတွင်ကုဒ်ဖြင့်ပြောင်းလဲခြင်း ဥပမာ- VPN

သယ်ယူပို့ဆောင်ရေး အလွှာတွင်ကုဒ်ဖြင့်ပြောင်းလဲခြင်းအတွက် နောက်ထပ် ဥပမာတစ်ခုကတော့ Virtual Private Network (VPN) ဖြစ်ပါတယ်။ VPN မပါဘဲ အင်တာနက်သုံးမယ်ဆိုရင် အင်တာနက်ဝန်ဆောင်မှုပေးသူ (ISP) ရဲ့ ချိတ်ဆက်မှုလမ်းကြောင်းပေါ်ကနေ သင့်ဒေတာတွေဖြတ်စီးပါတယ်။ VPN သုံးမယ်ဆိုရင်တော့ သင့်ဒေတာတွေက ISP ချိတ်ဆက်မှုလမ်းကြောင်း ပေါ် ဖြတ်စီးရင်တောင် သင်နဲ့ သင့် ISP အကြားမှာ ကုဒ်ဖြင့်ပြောင်းလဲခြင်းကို လုပ်ပေးထားမှာပါ။ တစ်စုံတစ်ယောက်က သင့်ရဲ့ ကိုယ်ပိုင်ချိတ်ဆက်မှုကွန်ယက်ကနေ သင့်ဘယ်ဝက်ဘ်ဆိုက်တွေကို ဝင်ရောက်လေ့ဆိုတာကို စောင့်ကြည့်ထောက်လှမ်းတဲ့အခါ VPN ကို အသုံးပြုထားမယ်ဆိုရင် သင်ဘယ် ဝက်ဘ်ဆိုက်ကို ဝင်နေလဲဆိုတာကို သိရမှာမဟုတ်ပါဘူး။ သင့် ISP ကတော့ သင်ဘယ် VPN ကို သုံးလဲ ဆိုတာကိုသိနေမှာပါ။

VPN ကိုသုံးလိုက်တဲ့အခါ သင့် ISP က သင်ဘယ်ဆိုက်တွေကိုဝင်နေလဲဆိုတာမသိနိုင်ပေမယ့် VPN ဝန်ဆောင်မှုပေးသူတွေကတော့ အဲ့ဒီအချက်အလက်တွေကို တွေ့မြင်နေရမှာပါ။ VPN ဝန်ဆောင်မှုပေးသူအနေနဲ့ သင့်ရဲ့ အင်တာနက်အသုံးပြုမှုဆိုင်ရာ အချက်အလက်တွေကို မြင်ရမယ်၊ သိမ်းဆည်းထားနိုင်တဲ့အပြင် ဒေတာစီးဆင်းမှုကိုပါ ပုံစံပြောင်းလို့ရပါတယ်။ အတိုပြောရရင် ISP ထက် VPN ဝန်ဆောင်မှုပေးသူကို ပိုယုံကြည်တဲ့သဘောပေါ့။ ဒါ့ကြောင့် သင်သုံးတဲ့ VPN က အချက်အလက်လုံခြုံမှုကို အာမခံပေးနိုင်တဲ့ VPN ဖြစ်ဖို့လိုပါတယ်။

မှန်ကန်တဲ့ VPN ကိုရွေးချယ်အသုံးပြုနိုင်ဖို့ ဒီလမ်းညွှန်တွေ read SSD's guide ကိုဖတ်ရှုပါ။

အစ - အဆုံးကုဒ်ဖြင့်ပြောင်းလဲခြင်း



ဒီပုံကားချပ်က အစ-အဆုံးကုဒ်ဖြင့်ပြောင်းလဲခြင်းကို ဆွဲပြထားတာပါ။ ဘယ်ဘက်က စမတ်ဖုန်းကနေ ကုဒ်နဲ့ပြောင်းလဲမထားတဲ့ “ဟဲလို”ဆိုတဲ့အစိမ်းရောင်မက်ဆေ့ချ်ကို ပို့လိုက်ပါတယ်။ အဲဒီမက်ဆေ့ချ်ကို ကုဒ်နဲ့ပြောင်းလဲပြီး ဖုန်းတာဝါနဲ့ ကုမ္ပဏီတာဝါတွေကိုဖြတ်စီးစေပါတယ်။ နောက်ဆုံးမှာတော့ ကုဒ်နဲ့ပြောင်းလဲထားတဲ့မက်ဆေ့ချ်က လက်ခံသူရဲ့ စမတ်ဖုန်းကို ရောက်ရှိသွားတဲ့အခါမှ ပြန်ဖြည်ပေးပြီး “ဟဲလို” လို့ မြင်ရပါမယ်။ သယ်ယူပို့ဆောင်ရေးအလွှာတွင် ကုဒ်ဖြင့်ပြောင်းလဲခြင်းနည်းလမ်းနဲ့ ကွာခြားတာတစ်ခုကတော့ သင့် ISP ဆာဗာတွေမှာ မက်ဆေ့ချ်ကို ပြန်ဖြည်လို့ decrypt လို့မရနိုင်ပါဘူး။ စမှတ်နဲ့ ဆုံးမှတ်ဖြစ်တဲ့ ပေးပို့သူနဲ့ လက်ခံသူနှစ်ဦးမှာသာ ပြန်ဖြည်နိုင်တဲ့သော့တွေရှိပါတယ်။

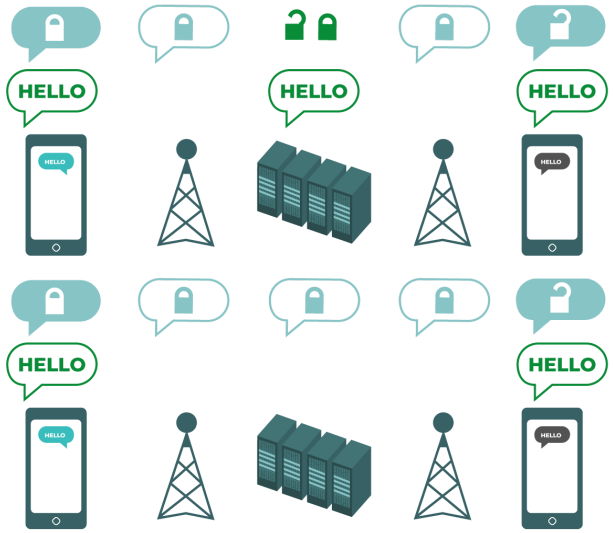
အစ - အဆုံးကုဒ်ဖြင့်ပြောင်းလဲခြင်းနည်းလမ်းက ပေးပို့သူနဲ့လက်ခံသူအကြား မက်ဆေ့ချ်သွားရာလမ်းတလျှောက်လုံးမှာ အကာအကွယ်ပေးပါတယ်။ မက်ဆေ့ချ်စတင်ပေးပို့လိုက်တာနဲ့ ကုဒ်နဲ့ပြောင်းလဲလိုက်ပြီး ဝှက်စာဖြစ်သွားစေပါတယ်။ အဲဒီဝှက်စာကို နောက်ဆုံးလက်ခံသူကသာ ပြန်ဖြည်ပြီး ကြည့်ရှုလို့ရပါတယ်။ အက်ပ်ဝန်ဆောင်မှုပေးသူတွေအပါအဝင် ဘယ်သူကမှသင့်ရဲ့လုပ်ဆောင်ချက်တွေကို စောင့်ကြည့်နားထောင်လို့မရပါဘူး။

အက်ပ်တစ်ခုမှာ အစ - အဆုံးကုဒ်ဖြင့်ပြောင်းလဲခြင်းကိုသုံးပြီး မက်ဆေ့ချ်တွေပေးပို့တဲ့အခါ အဲဒီ အက်ပ်ကုမ္ပဏီကိုယ်တိုင်က မက်ဆေ့ချ်တွေကို ဖတ်လို့မရပါဘူး။ ဒီလုပ်ဆောင်ချက်က ကုဒ်ဖြင့် ပြောင်းလဲခြင်း encryption အတွက် အဓိကရှိရမဲ့ အရည်အသွေးလည်းဖြစ်ပါတယ်။ စဉ်းစားကြည့်ရင် ဒီအက်ပ်ကို

ဒီဇိုင်းလုပ်ပြီး စီမံခန့်ခွဲသူတွေကိုယ်တိုင်က ကုဒ်ကိုပြန်ဖြည်ဖို့မဖြစ်နိုင်တော့ သိပ်ပြောင်မြောက်တဲ့ လုပ်ဆောင်ချက်လို့ ဆိုနိုင်တာပေါ့။

စောင့်ကြည်ထောက်လှမ်းမှုအတွက်ကိုယ်ပိုင်ခုခံကာကွယ်ခြင်း လမ်းညွှန်တွေမှာ အစ - အဆုံးကုဒ်ဖြင့်ပြောင်းလဲခြင်း အတွက်အသုံးပြုနိုင်တဲ့ နည်းစနစ်တွေကို Communicating With Others လမ်းညွှန်မှာ ကြည့်လို့ရပါတယ်။

သယ်ယူပို့ဆောင်ရေးအလွှာတွင် ကုဒ်ဖြင့်ပြောင်းလဲခြင်း (သို့မဟုတ်) အစ - အဆုံးကုဒ်ဖြင့်ပြောင်းလဲခြင်းနှစ်ခုမှာ ဘယ်နည်းလမ်းကို ရွေးချယ်ရမလဲ။

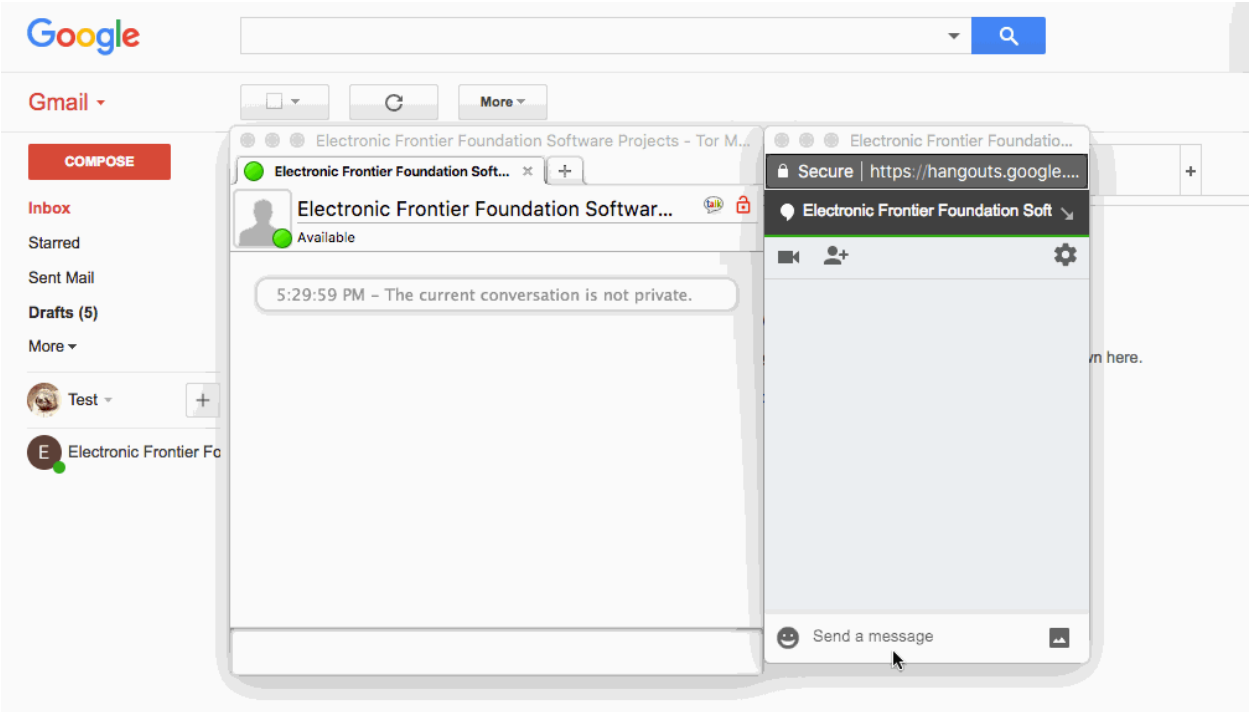


သယ်ယူပို့ဆောင်ရေးအလွှာတွင် ကုဒ်ဖြင့်ပြောင်းလဲခြင်း (သို့မဟုတ်) အစ - အဆုံးကုဒ်ဖြင့်ပြောင်းလဲခြင်းနှစ်ခုမှာ ဘယ်နည်းလမ်းကို ရွေးချယ်ရမလဲဆိုတာကို ဆုံးဖြတ်ဖို့ ဒီမေးခွန်းလေးတွေကို အရင်ဖြေကြည့်ပါ။ သင့်သုံးတဲ့ အက်ပ် (သို့မဟုတ်) ဝန်ဆောင်မှုအပေါ် ယုံကြည်မှုရှိသလား။ အဲဒါတွေရဲ့ နည်းပညာတွေကို ယုံကြည်သလား။ တရားဥပဒေဆိုင်ရာအဖွဲ့အစည်းတွေရဲ့ တောင်းဆိုမှုတွေနဲ့ ပတ်သက်လို့ အဲဒီကုမ္ပဏီတွေရဲ့ ပေါ်လစီတွေကရော ဘယ်လိုရှိသလဲ။

အဲဒီမေးခွန်းတွေရဲ့ အဖြေက “ဟင့်အင်း” ဆိုရင်တော့ အစ - အဆုံးကုဒ်ဖြင့်ပြောင်းလဲခြင်းနည်းလမ်းကို ရွေးချယ်ပါ။ တကယ်လို့ သင့်အဖြေက “အင်း” ဆိုရင်တော့ သယ်ယူပို့ဆောင်ရေးအလွှာတွင် ကုဒ်ဖြင့်

ပြောင်းလဲခြင်းနည်းလမ်းလောက်နဲ့ အဆင်ပြေနိုင်ပါတယ်။ ဒါပေမဲ့လည်း အစ - အဆုံး ကုဒ်ဖြင့်ပြောင်းလဲခြင်းနည်းလမ်းကိုသုံးတဲ့ ဝန်ဆောင်မှုတွေကတော့ ပိုစိတ်ချရတာမို့ ရွေးချယ်သင့်ပါတယ်။

အစ - အဆုံးကုဒ်ဖြင့် ပြောင်းလဲခြင်း နဲ့ သယ်ယူပို့ဆောင်ရေးအလွှာတွင် ကုဒ်ဖြင့်ပြောင်းလဲခြင်း ဘယ်လို အလုပ်လုပ်သလဲဆိုတာကို အောက်မှာသရုပ်ပြပေးထားပါတယ်။ ဘယ်ဘက်ကတော့ အစ - အဆုံး ကုဒ်ဖြင့် ပြောင်းလဲခြင်းကို အသုံးပြုတဲ့ chat tool (Off-the-Record ("OTR") ဆိုတဲ့ ပို့တဲ့ မက်ဆေ့ချ်ကို ချက်ချင်းကုဒ်ဖြင့်ပြောင်းလဲနိုင်တဲ့ ချက်ဘောက်စ်)ဖြစ်ပါတယ်။ ညာဘက်ကတော့ သယ်ယူပို့ဆောင်ရေးအလွှာတွင် ကုဒ်ဖြင့်ပြောင်းလဲခြင်းကို အသုံးပြုတဲ့ ချက်ဘောက်စ် (HTTPS ကိုသုံးတဲ့ Google Hangouts' ဝက်ဘက်ဆိုက်ကိုသုံးပြီး ကုဒ်ဖြင့်ပြောင်းလဲခြင်းလုပ်တဲ့ ချက်ဘောက်စ်) ဖြစ်ပါတယ်။



ပထမလူက ဒီ GIF မှာ Google Hangouts ရဲ့ ချက်ဘောက်စ်မှာ မက်ဆေ့ချ်တစ်ခုကို ရိုက်လိုက်ပါတယ်။

"ဟိုင်း ဒီဟာက အစ - အဆုံး ကုဒ်ဖြင့်ပြောင်းလဲထားတာမဟုတ်လို့ ဂူဂယ်လ်က ငါတို့ပြောနေတာတွေကို မြင်နေရတယ်" လို့အဓိပ္ပါယ်ရှိတဲ့ အင်္ဂလိပ်စာကြောင်းကို ရိုက်ထားပါတယ်။

အသုံးပြုသူက Off-the-Record (OTR) ချက်ဘောက်စ်ကိုလည်းဖွင့်ထားပြီး ဆက်တင်မှာ “private conversation” လုပ်ဆောင်ချက်ကိုဖွင့်ထားပါတယ်။ OTR ချက်ဘောက်စ်မှာ ရှင်းလင်းချက်ကို ဒီလို ရေးထားပါတယ်။

“[gmail account] နဲ့ သီးသန့်စကားပြောဖို့ လုပ်ဆောင်နေပါတယ်။ [gmail account] နဲ့ သီးခြား စကားစ ပြောနေပါပြီ။ ဒါပေမဲ့ ဘယ်သူနဲ့ဘယ်သူပြောနေတယ်ဆိုတာကို မသိနိုင်ပါဘူး” လို့အဓိပ္ပါယ်ရှိတဲ့ အင်္ဂလိပ်စာကြောင်းကိုရိုက်ထားပါတယ်။

တပြိုင်နက်ထဲမှာပဲ Google Hangouts ချက်ဘောက်စ်မှာ ဘယ်သူမှဖတ်လို့မရတဲ့ ဝှက်စာကြောင်းတစ်ခုကို ပို့လိုက်တာကို တွေ့ရပါတယ်။ ဒါကဘာကိုပြသလဲဆိုရင် Off-the-Record (OTR) ကို အသုံးပြုတဲ့ အစ - အဆုံးကုဒ်ဖြင့်ပြောင်းလဲခြင်းကို အသုံးပြုပြီး ဆက်သွယ်နေတယ်လို့ ဖော်ပြတာဖြစ်ပါတယ်။ OTR ချက်ဘောက်စ်မှာရေးထည့်တဲ့ မက်ဆေ့ချ်တိုင်းက Google Hangouts ချက်ဘောက်စ် မှာ ဖတ်မရတဲ့စာတွေအဖြစ် ပေါ်လာပါတယ်။ အောက်ကစာကြောင်းကို ဒုတိယလူက စာပြန်ရိုက်ပို့ပါတယ်။

“ဒီစာတွေအားလုံးကို သူများတွေဖတ်လို့မရဘူး” လို့ပြောပါတယ်။

တခါပထမလူက -

“ဟုတ်ပ။ အဓိပ္ပါယ်မရှိတဲ့စာတွေပဲ” လို့ ပြန်ပြောပါတယ်။

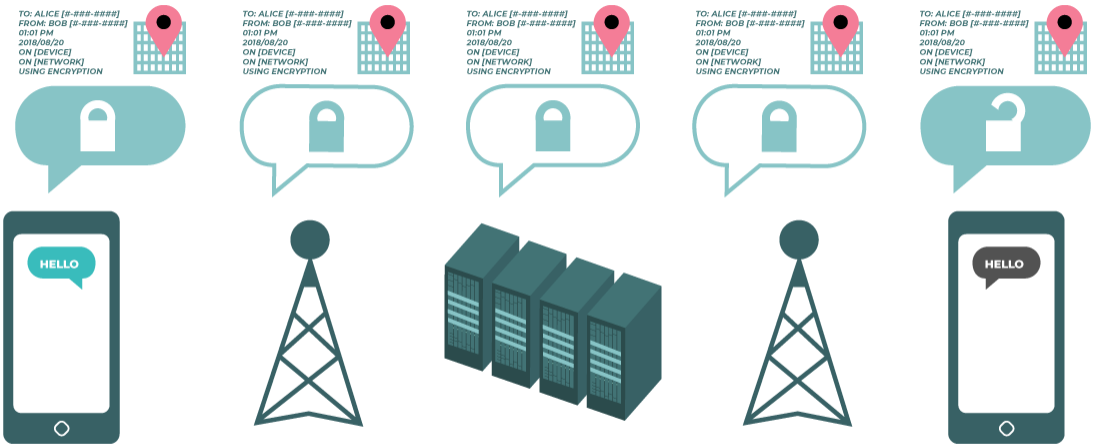
ဒုတိယလူက ပြုံးနေတဲ့ အီမိုဂျီလေးပို့ပေးလိုက်တယ်။

သယ်ယူပို့ဆောင်ရေးအလွှာတွင် ကုဒ်ဖြင့်ပြောင်းလဲခြင်း မှာ ဘာလုပ်ဆောင်ချက်တွေမပါဘူးလဲ။

ကုဒ်ဖြင့်ပြောင်းလဲခြင်းက အရာအားလုံးကို အဖြေမထုတ်ပေးနိုင်ပါဘူး။ သင့်အနေနဲ့ ကုဒ်နဲ့ပြောင်းလဲထားတဲ့ မက်ဆေ့ချ်တွေကို ပို့တယ်ဆိုရင်တောင် သင်ပို့လိုက်တဲ့သူဆီမှာအဲဒါတွေကို ပြန်ဖြည်မှာပါ။ ပို့တဲ့သူနဲ့ လက်ခံတဲ့သူတွေသုံးတဲ့ စက်ပစ္စည်းတွေမှာ လုံခြုံရေးကျိုးပေါက်နေရင် သင်တို့ရဲ့ ပြောဆို တက်သွယ်မှုတွေကလည်း လုံခြုံမှုရှိမှာမဟုတ်ပါဘူး။ ဒါ့အပြင် သင့်တို့ပြောကြားနေတာတွေကို လက်ခံသူက စခရင်ရှော့ရိုက်ယူပြီးသိမ်းတာ ဒါမှမဟုတ် သင်တို့ဆက်သွယ်မှုတွေကို မှတ်တမ်းယူထားတာမျိုးတွေလည်း ဖြစ်နိုင်ပါသေးတယ်။

သင့်အနေနဲ့ သင်ပြောဆိုဆက်သွယ်သမျှတွေကို “cloud” ပေါ်မှာ အလိုအလျောက် ပုံတူပွားသိမ်းဆည်းထားတယ်ဆိုရင် အဲဒီပုံတူပွားအချက်အလက်တွေကိုလည်း ကုဒ်နဲ့ပြောင်းလဲပြီးမှသိမ်းဆည်းဖို့ သတိပြု

ပါ။ ဒီလိုလုပ်ခြင်းအားဖြင့် အထိုင်သိမ်းထားတဲ့အချိန်မှာရော ဟိုဘက်ဒီဘက် အပြန်အလှန်ပို့ချိန်မှာရော သင့်ဒေတာတွေ လုံခြုံမှုရှိမှာပါ။



သင့်အနေနဲ့ ဒေတာ data တွေစီးဆင်းနေတဲ့အချိန်မှာ ကုဒ်နဲ့ပြောင်းလဲခြင်း encrypt ကို သုံးမယ်ဆိုရင် သင့်ရဲ့ ဆက်သွယ် ပြောဆိုရာမှာပါဝင်နေတဲ့ အချက်အလက်တွေအားလုံးကို ကာကွယ်ပေးနိုင်ပေမဲ့ သင့်ရဲ့ အချက်အလက်အကြောင်းရှင်းပြတဲ့ အချက်အလက်တွေဖြစ်တဲ့ metadata ကိုတော့ ကုဒ်နဲ့ပြောင်းလဲ ပေးမှာမဟုတ်ပါဘူး။ ဥပမာ - သင်နဲ့ သင့်သူငယ်ချင်းအကြားအပြန်အလှန်ပို့ထားတဲ့ မက်ဆေ့ချ်တွေကို ဖတ်မရအောင်လုပ်ပေးထားပေမဲ့ အောက်ကအချက်တွေကိုတော့ ကွယ်ဝှက်ပေးထားမှာမဟုတ်ပါဘူး။

- သင်နဲ့သင့်သူငယ်ချင်းအကြား ဆက်သွယ်ပြောဆိုမှုတွေရှိနေတယ်ဆိုတာ
- သင်တို့တွေဟာ ကုဒ်ဖြင့်ပြောင်းလဲခြင်းကိုသုံးပြီ ်းဆက်သွယ်နေတယ်ဆိုတာနဲ့
- အခြားအချက်အလက်တွေဖြစ်တဲ့ ဆက်သွယ်ပြောဆိုမှုတွေမှာ သင်တို့ရဲ့ တည်နေရာ၊ အချိန်နဲ့ ကြချိန်တွေကိုတော့ မှတ်တမ်းရှိနေမှာပါ။

လုံခြုံရေးကိုမြှင့်ထားချင်တဲ့သူတွေ (ဥပမာ - မိမိရဲ့ချိတ်ဆက်ဆောင်ရွက်မှုတွေကို စောင့်ကြည့်ခံရမှာ စိုးရိမ်သူတွေ) အနေနဲ့ အရေးကြီးတဲ့အချိန်တွေမှာပဲ ကုဒ်ဖြင့်ပြောင်းလဲခြင်းကို အသုံးပြုတာ အန္တရာယ်များပါတယ်။ ဆိုလိုတာက သင့်အနေနဲ့ အရေးကြီးချိန် ဒါမှမဟုတ် တချို့ကိစ္စတွေအတွက်ပဲ ကုဒ်ဖြင့်ပြောင်းလဲခြင်းကို သုံးတာကြောင့် သင့် အချက်အလက်တွေအကြောင်းဖော်ပြတဲ့ အချက်အလက်တွေ ဖြစ်တဲ့ metadata မှာပေါ်နေတဲ့ အရေးကြီးတဲ့ အချိန်နဲ့နေရာတွေနဲ့ ချိန်ကိုက်ပြီး တိုက်စစ်လို့ရပါ တယ်။ ဒါ့ကြောင့် ဘယ်အချိန်၊ ဘယ်နေရာမှာ ဘာပဲလုပ်လုပ် ကုဒ်နဲ့ပြောင်းလဲခြင်းကို တတ်နိုင်သမျှ သုံးပါ။

နောက်တစ်ချက်က ကုဒ်ဖြင့်ပြောင်းလဲခြင်းကို အသုံးပြုတဲ့ နက်ဝေါ့ခ်မှာ အသုံးပြုသူကသင်တစ်ယောက်တည်းဖြစ်နေရင် သံသယဝင်စရာဖြစ်ပါလိမ့်မယ်။ ဒါ့ကြောင့် ကုဒ်နဲ့ပြောင်းလဲခြင်းကို လူတိုင်းအသုံးပြုဖို့နှိုးဆော်ကြတာပါ။ လူတိုင်းကသုံးနေမယ်ဆိုရင် ဒါက ပုံမှန်လုပ်ရိုးလုပ်စဉ်ဖြစ်သွားပြီး သံသယဝင်ကြတော့မှာမဟုတ်ပါဘူး။ တကယ်လိုတဲ့သူအတွက်လည်း အထောက်အကူအကြီးကြီး ရတာပေါ့။

ဇာတ်ပေါင်းသော်

အထိုင်ဒေတာရော ရွှေ့လျားဒေတာ နှစ်မျိုးလုံးကို ကုဒ်နဲ့ပြောင်းလဲခြင်းလုပ်ထားတာက တစ်ခုတည်းအတွက်သုံးတာထက်ပိုပြီး စိတ်ချလုံခြုံမှုရစေပါတယ်။ ဒါကို လုံခြုံရေးဆိုင်ရာ ကျွမ်းကျင်သူတွေက “ခိုင်မာသောကာကွယ်မှုစနစ်” လို့ ဆိုကြပါတယ်။ အမျိုးမျိုးသော နည်းလမ်းတွေကိုသုံးပြီးသင့်ဒေတာကိုကာကွယ်ထားခြင်းကြောင့် သင့်အနေနဲ့ ပိုမိုစိတ်ချရတဲ့ ကာကွယ်မှုမျိုးကို ရရှိစေမှာပါ။

ဥပမာပြောရရင် သင့်အနေနဲ့ ကုဒ်နဲ့ပြောင်းလဲထားခြင်းမရှိတဲ့ မက်ဆေ့ချ် (ကုဒ်နဲ့ပြောင်းလဲမထားတဲ့ ရွှေ့လျားဒေတာ) ကို ကုဒ်နဲ့ပြောင်းလဲထားတဲ့ စက်ပစ္စည်း (ကုဒ်နဲ့ပြောင်းလဲထားတဲ့အထိုင်ဒေတာ) က နေပို့မယ်ဆိုရင် သင့်မက်ဆေ့ချ်ကို ကြားဖြတ်ခိုးယူစောင့်ကြည့်မယ့်သူတွေဖြစ်တဲ့ အစိုးရ၊ ဝန်ဆောင်မှုပေးသူတွေ (သို့မဟုတ်) နည်းပညာကျွမ်းကျင်တဲ့ ဒေတာသူခိုးတွေရန်ကနေ ကာကွယ်နိုင်မှာမဟုတ်ပေမဲ့

သင့်မိုဘိုင်းစက်ပစ္စည်းကို ကိုယ်ထိလက်ရောက်ဝင်ရောက် ခိုးယူနိုင်သူတွေဆီမှာ စကားဝှက် မရှိသရွေ့ အဲဒီထဲမှာ သိမ်းဆည်းထားတဲ့ မက်ဆေ့ချ်တွေကိုတော့ ကာကွယ်ပေးနိုင်မှာပါ။

အပြန်အလှန်ပါပဲ။ သင့်အနေနဲ့ အစ - အဆုံးကုဒ်ဖြင့်ပြောင်းလဲထားတဲ့ မက်ဆေ့ချ် (ကုဒ်နဲ့ပြောင်းလဲထားတဲ့ ရွေ့လျားဒေတာ) ကို ကုဒ်နဲ့ပြောင်းမလဲထားတဲ့ စက်ပစ္စည်း (ကုဒ်နဲ့ပြောင်းမလဲထားတဲ့အထိုင်ဒေတာ) ကနေ ပို့မယ်ဆိုရင် သင့်မက်ဆေ့ချ်ပို့ချိန်မှာ ဘယ်သူမှစောင့်ကြည့်ခိုးယူလို့မရပေမဲ့ သင့်မိုဘိုင်းစက်ပစ္စည်းကို တစ်စုံတစ်ယောက်က ရယူသွားမယ်ဆိုရင် သင့်ရဲ့ မက်ဆေ့ချ်တွေကို ဖတ်လို့ရသွားမှာပါပဲ။

ဒီဥပမာတွေကို စိတ်ထဲမှာစွဲစွဲမြဲမြဲမှတ်သားပြီး သင့်ဒေတာတွေကို အထိုင်အခြေအနေရော၊ ရွေ့လျားအခြေအနေနှစ်မျိုးလုံးမှာ ကုဒ်နဲ့ပြောင်းလဲခြင်းကိုလုပ်ထားခြင်းက သင့်အတွက် အကောင်းဆုံးအကာအကွယ်ဆိုတာကို အမြဲတမ်းအမှတ်ရပါ။

ကုဒ်ဖြင့်ပြောင်းလဲခြင်းကို ဘယ်လိုအသုံးပြုရမလဲဆိုတာနဲ့ပတ်သက်လို့ Key Concepts in Encryption လမ်းညွှန်မှာ ဆက်လက်လေ့လာပါ။