EFF'S SURVEILLANCE SELF-DEFENSE

ကုန်ဖြင့် ကြောင်းလဲခြင်းဆိုင်ရာ အခြေခံအယူအဆများ

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

LOCALIZATION LAB

ကုဒ်ဖြင့် ပြောင်းလဲခြင်းဆိုင်ရာ အခြေခံအယူအဆများ

နောက်ဆုံးစိစစ်သည့်ရက်စွဲ- ၂၈/၀၆/၂၀၂၁

အများအားဖြင့် ကုဒ်ဖြင့်ပြောင်းလဲခြင်းက အသုံးပြုရတာ ရိုးရှင်းပါတယ်။ ဒါပေမဲ့လည်း တခါတရံမှာတော့ အမှားအယွင်းတွေ ဖြစ်တတ်ပါတယ်။ သူ့အကြောင်းကို ပိုနားလည်လေလေ အမှားအယွင်းဖြစ်နိုင်ချေ နည်းလေလေပါ။ ဒါ့ကြောင့် ကုဒ်ဖြင့်ပြောင်းလဲခြင်းနဲ့ ပတ်သက်လို့ ဘာတွေသိထားသင့်လဲ ဆိုတာကို ရေးထားတဲ့လမ်းညွှန် ကုတ်ဖြင့်ပြောင်းလဲခြင်းအကြောင်း ဘာတွေသိသင့်သလဲကို ဖတ်ဖို့ အကြံပြုပါတယ်။

ဒီလမ်းညွှန်မှာတော့ အိုင်ဒီယာငါးခုအကြောင်း ရှင်းပြပါမယ်။ ဒီအိုင်ဒီယာတွေက ရွေ့လျားဒေတာတွေကို ကုဒ်နဲ့ပြောင်းလဲခြင်းအတွက် သိထားသင့်တဲ့ အခြေခံအယူအဆတွေ ဖြစ်ပါတယ်။

- ဆိုက်ဖာ၊ သော့
- ဘက်ညီနှင့် ဘက်မညီ ကုဒ်ဖြင့်ပြောင်းလဲခြင်း
- ကိုယ်ပိုင်နှင့် အများသုံး စကားဝှက်သော့များ
- လူအများ၏ ကိုယ်ရေးအချက်အလက် မှန်ကန်မှုကို အတည်ပြုခြင်း (အများသုံးစကားဝှက်သော့လက်မှေများ)
- ဝက်ဘ်ဆိုက်များ၏ အချက်အလက်မှန်ကန်မှုကို အတည်ပြုခြင်း (လုံခြုံရေးလက်မှတ်များ)

ဝှက်စာပုံသေနည်း၊ သော့

သင့်အနေနဲ့ အခြားဘာသာတစ်ခုနဲ့ရေးထားသလို၊ ဖတ်မရတဲ့စာတွေလိုလို ရေးထားတာ မြင်ဖူးပါလိမ့်မယ်။ အဲဒီစာတွေကို နားလည်နိုင်ဖို့အတွက် အတားအဆီးတစ်ခုခုနဲ့ ပိတ်ပင်ထားသလို ဖြစ်နေတတ်ပါတယ်။ ဒါပေမဲ့ အဲ့ဒီလိုရေးထားတဲ့ စာတိုင်းက ကုဒ်ဖြင့်ပြောင်းလဲထားတာ မဟုတ်ပါဘူး။

နားမလည်အောင်ရေးထားတဲ့စာနဲ့ ကုဒ်နဲ့ပြောင်းလဲထားတဲ့ စာနှစ်မျိုးကို ဘယ်လိုခွဲခြားမလဲ။

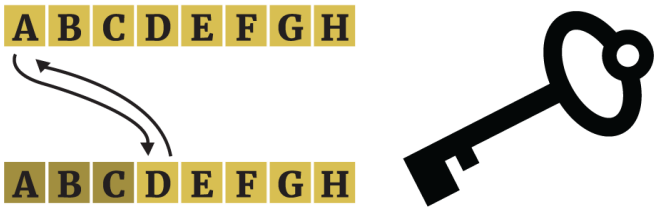
ကုဒ်ဖြင့်ပြောင်းလဲခြင်း ဆိုတာ သတင်းအချက်အလက်ကို ပုံဖျက်ပြီး တိကျတဲ့ နည်းလမ်းတစ်ခုနဲ့ ပြန်ဖြည်တဲ့ သခ်ၤာနည်းလမ်းဖြစ်စဉ် တစ်ခု ပါ။ ဒီဖြစ်စဉ်မှာ ဆိုက်ဖာနဲ့ သော့ပါဝင်ပါတယ်။

ဝှက်စာပုံသေနည်း ဆိုတာ ကုဒ်ဖြင့်ပြောင်းလဲခြင်းနဲ့ ပြန်ဖြည်ခြင်းတို့အတွက် လိုက်နာဆောင်ရွက်ရတဲ့ အဆင့်တွေကိုရေးထားတဲ့ အယ်ဂိုရစ်သမ် (algorithm) ဖြစ်ပါတယ်။ ဒီတိကျရှင်းလင်းလှတဲ့အဆင့်တွေကို ဖော်မြူလာပုံသေနည်း တစ်ခုလို လိုက်နာနိုင်ပါတယ်။

စကားဝှက်သော့ ဆိုတာကတော့ ဝှက်စာပုံသေနည်းမှာ ကုဒ်ဖြင့်ပြောင်းလဲခြင်းနဲ့ ပြန်ဖြည်ခြင်းကို ဘယ်လို လုပ်မလဲ ဆိုတာကို ညွှန်ကြားတဲ့ သတင်းအချက်အလက်အပိုင်းအစ ဖြစ်ပါတယ်။ သော့တွေဟာ ကုဒ်ဖြင့်ပြောင်းလဲခြင်းကို နားလည်ဖို့အတွက် မသိမဖြစ် သိထားရမယ့် အခြေခံအယူအဆတွေထဲက တစ်ခုလည်း ဖြစ်ပါတယ်။

စကားဝှက်သော့ တစ်ချောင်းတည်း သုံးမလား၊ စကားဝှက်သော့ အများကြီး သုံးမလား။

ဘက်ညီကုဒ်ဖြင့်ပြောင်းလဲခြင်း စနစ်မှာ ကုဒ်ဖြင့်ပြောင်းလဲခြင်းနဲ့ ပြန်ဖြည်ခြင်းဖြစ်စဉ် နှစ်ခုလုံး အတွက် စကားဝှက်သော့တစ်ချောင်းတည်း လိုပါတယ်။



အစောပိုင်းမှာသုံးခဲ့တဲ့ ကုဒ်ဖြင့်ပြောင်းလဲခြင်းတွေက ဘက်ညီစနစ်တွေ ဖြစ်ပါတယ်။ ဂျူးလီးယက်ဆီဇာသုံးခဲ့တဲ့ “ဆီဇာဝှက်စာပုံသေနည်း” ဆိုရင် သုံးလုံးမြောက်အက္ခရာကို အစားထိုးတဲ့ ပုံသေနည်းကို ဝှက်စာရေးဖို့နဲ့ ပြန်ဖြည်ဖို့အတွက် သုံးပါတယ်။ ဥပမာအားဖြင့် A နေရာမှာ D နဲ့ အစားထိုးထားတာပါ။ ဒီပုံသေနည်းကိုသုံးပြီး “ENCRYPTION IS COOL” ဆိုတဲ့ မက်ဆေ့ချ်ကို ရေးရင် “HQFUBSWLRQ LV FRRO” ဒီလိုပုံစံ မြင်ရမှာပါ။ တူညီတဲ့ပုံသေနည်းကို အသုံးပြုပြီး ဝှက်စာကိုပြန်ဖြည်နိုင်ပါတယ်။

ဘက်ညီကုဒ်ဖြင့်ပြောင်းလဲခြင်း နည်းလမ်းကို ယခုအချိန်အထိ အသုံးပြုနေဆဲပါ။ ဒါပေမဲ့ ပိုပြီးရှုပ်ထွေးပြီး ပြန်ဖြည်ရခက်တဲ့ သင်္ချာနည်းလမ်းတွေနဲ့ တည်ဆောက်ထားတဲ့ “stream ciphers” နဲ့ “block ciphers” ပုံစံမျိုးနဲ့ အသုံးပြုကြပါတယ်။ အခုခေတ်သုံး ကုဒ်ဖြင့်ပြောင်းလဲခြင်း နည်းစနစ်တွေမှာ ဒေတာတွေကို ပြောင်းလဲတဲ့အဆင့်တွေ အများကြီးပါဝင်တာမို့ သော့မရှိရင် ပြန်ဖြည်ဖို့ မလွယ်ပါဘူး။ Advanced Encryption Standard (AES) algorithm လိုမျိုး ခေတ်ပေါ်ဘက်ညီကုဒ်ပြောင်းလဲ

ခြင်းအယ်လ်ဂိုရစ်သမ်တွေက မြန်ဆန်ပြီးစိတ်ချရပါတယ်။ ဘက်ညီကုဒ်ဖြင့်ပြောင်းလဲခြင်း နည်းစနစ် ကို ဖိုင်များအားကုဒ်ဖြင့်ပြောင်းလဲခြင်း၊ ကွန်ပျူတာထဲမှာ ကုဒ်ဖြင့်ပြောင်းလဲခြင်းအတွက် အကန့်များ ခွဲခြင်း၊ စက်ပစ္စည်းတစ်ခုလုံးကို ကုဒ်ဖြင့်ပြောင်းလဲခြင်း၊ ကွန်ပျူတာများတွင် အပြည့်အဝကုဒ်ဖြင့် ပြောင်းလဲခြင်းနဲ့ ဗွက်စာမန်နေဂျာတွေသုံးပြီး ဒေတာဘေ့စ်တွေကို ကုဒ်ဖြင့် ပြောင်းလဲခြင်း စတာတွေအတွက် တွင်တွင်ကျယ်ကျယ်အသုံးပြုကြပါတယ်။ ဒီလို ဘက်ညီကုဒ်ဖြင့် ပြောင်းလဲထားတဲ့ဗွက်စာတွေကို ပြန်ဖြည်တဲ့အခါ စကားဝှက်ကို အသုံးပြုရလေ့ရှိတာမို့ ခိုင်မာအားကောင်းတဲ့စကားဝှက်တွေကို အသုံးပြုဖို့ နဲ့ အဲဒီလိုစကားဝှက်တွေကို ဖန်တီးနိုင်ဖို့ လမ်းညွှန်တွေကို ဖတ်ဖို့ အကြံပြုတာပါ။

စကားဝှက် သော့တစ်ချောင်းတည်း ရှိတာ ဘာတစ်ခုကောင်းလဲ ဆိုတော့ သင်ကလွဲလို့ ဘယ်သူ့ဆီမှာမှ အဲဒီသော့ မရှိဘူးဆိုတာပါပဲ။ ဒါပေမဲ့ ပြဿနာတစ်ခုရှိနေပါတယ်။ အဲဒီသော့ကို အဝေးမှာရှိတဲ့ မိတ်ဆွေတစ်ယောက်ထံ ပို့ချင်ရင်ဘယ်လိုလုပ်မလဲ။ သင့်မိတ်ဆွေကို သီးခြားတွေ့ဆုံလို့ မရတဲ့ အခြေအနေမျိုးမှာ သော့ကို ဘယ်လိုပို့ပေးမလဲ။ အင်တာနက်ထဲကနေ အဲဒီသော့ကို လုံလုံခြုံခြုံ ဘယ်လိုပို့ပေးမလဲ။

ဘက်မညီကုဒ်ဖြင့်ပြောင်းလဲခြင်း ကို အများသုံးစကားဝှက်သော့ဖြင့် ကုဒ်ပြောင်းလဲခြင်း လို့လည်းခေါ်ကြပါတယ်။ ဒီနည်းစနစ်က ခုနဖော်ပြခဲ့တဲ့ ပြဿနာတွေကို ရှင်းနိုင်ပါတယ်။ ဘက်မညီကုဒ်ဖြင့်ပြောင်းလဲခြင်းမှာ ဗွက်စာဖြည်ဖို့အတွက် ကိုယ်ပိုင်စကားဝှက်သော့နဲ့ ကုဒ်ဖြင့်ပြောင်းလဲ ခြင်းလုပ်နိုင်ဖို့ အတွက် အများသုံးစကားဝှက်သော့ ဆိုပြီး စကားဝှက် သော့နှစ်ချောင်း ပါဝင်ပါတယ်။

ဘက်ညီကုဒ်ဖြင့်ပြောင်းလဲခြင်း	ဘက်မညီကုဒ်ဖြင့်ပြောင်းလဲခြင်း
• မြန်ဆန်	• နှေးကွေး
• ကွန်ပျူတာတွက်ချက်မှု ပါဝါသိပ်မလို	• ကွန်ပျူတာတွက်ချက်မှု ပါဝါ အများကြီးလိုအပ်
• မက်ဆေ့ချ် အရွယ်အစား အကြီးအငယ် အကုန် အတွက် အသုံးဝင်	• အရွယ်အစားသေးတဲ့ မက်ဆေ့ချ် များအတွက်သာ အသုံးဝင်
• ကုဒ်ဖြင့်ပြောင်းလဲခြင်း နှင့် ပြန်ဖြည်ခြင်းနှစ်မျိုးလုံး အတွက် သုံးတဲ့သော့ကို အခြားသူကိုပေးဖို့လို	• ပြန်ဖြည်ဖို့အတွက်သုံးတဲ့ စကားဝှက်သော့ကို အခြားသူထံ ပေးဖို့မလို၊ ကုဒ်နဲ့ ပြောင်းလဲခြင်းအတွက် သုံးတဲ့ အများသုံးစကားဝှက်သော့ကိုပဲ အခြားသူထံ ပေးဖို့လို
• အသုံးပြုသူတွေရဲ့ မည်သူမည်ဝါဖြစ်ကြောင်းမှန်ကန်မှုကို အတည်ပြု စစ်ဆေးနိုင်ခြင်း မရှိ	• အသုံးပြုသူတွေရဲ့ မည်သူမည်ဝါဖြစ်ကြောင်း မှန်ကန်မှုကို အတည်ပြု စစ်ဆေးနိုင်ခြင်းရှိ

ရွေးလျားဒေတာတွေကို ကုဒ်နဲ့ပြောင်းလဲရာမှာတော့ ဘက်ညီနဲ့ ဘက်မညီကုဒ်ဖြင့်ပြောင်းလဲခြင်းနှစ်မျိုးလုံးကို အတူ တွဲသုံးလေ့ ရှိပါတယ်။

ဘက်မည်ကုဒ်ဖြင့်ပြောင်းလဲခြင်း- သီးခြားနှင့် အများသုံး စကားဝှက်သော့ များ

ကိုယ်ပိုင်နှင့် အများသုံး စကားဝှက်သော့တွေဟာ တစ်စုံစီ လာပါတယ်။ အဲဒီသော့နှစ်ချောင်းကို သင်္ချာနည်းလမ်းနဲ့ ချိတ်တွဲထားပါတယ်။ ပြောရင်တော့ ကျောက်ခဲတစ်လုံးကို အလယ်တည့်တည့်ကနေ တခြမ်းစီခွဲထား သလိုပေါ့။ အဲဒီနှစ်ပိုင်းကို ပြန်ပေါင်းမှ တစ်ခုဖြစ်သလိုပါပဲ။ အခြားကျောက်တုံးက အပိုင်းကို သွားဆက်လို့ မရသလိုပေါ့။ ကိုယ်ပိုင်စကားဝှက်သော့နဲ့ အများသုံးစကားဝှက်သော့တွေမှာ ကွန်ပျူတာတွေကသာ ဖတ်နိုင်တဲ့ တူညီတဲ့ ကိန်းစဉ်အကြီးကြီးတွေ ပါဝင်ပါတယ်။

public

private

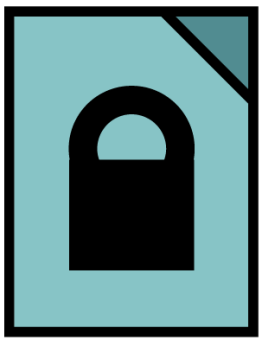
----- BEGIN PUBLIC KEY BLOCK -----

----- END PUBLIC KEY BLOCK -----

----- BEGIN PRIVATE KEY BLOCK -----

----- END PRIVATE KEY BLOCK -----

တကယ့်သော့အစစ်လိုမျိုး အရာဝတ္ထုတွေကို ဖွင့်တဲ့ လုပ်ဆောင်ချက် မလုပ်တဲ့ အတွက် “အများသုံး စကားဝှက်သော့” ဆိုတဲ့ အခေါ်အဝေါ်က နည်းနည်းတော့ စိတ်ရှုပ်စရာပါ။ သော့တွေနဲ့ ပတ်သက်လို့ အသေးစိတ်သိ ချင်ရင် တော့ အများသုံးစကားဝှက်သော့ပါ ဝှက်စာဖေဒအကြောင်း ထဲထဲဝင်ဝင်လေ့လာခြင်းမှာ ဝင်ရောက်လေ့လာ နိုင်ပါတယ်။



----- BEGIN PUBLIC KEY BLOCK -----

----- END PUBLIC KEY BLOCK -----

A public key is a file that you can give to anyone or publish publicly. When someone wants to send you an end-to-end encrypted message, they'll need your public key to do so.

အများသုံး စကားဝှက်သော့ဆိုတာက ဘယ်သူ့ဆီကိုမဆို လွတ်လွတ်လပ်လပ် မျှဝေလို့ရတဲ့ ဖိုင်ဖြစ်ပါတယ်။ တစ်စုံတစ်ယောက်က သင့်ဆီကို ကုဒ်ဖြင့်ပြောင်းလဲထားတဲ့ မက်ဆေချ်ကို ပို့ဖို့အတွက် သင့်ရဲ့ အများသုံးစကားဝှက်သော့ကို သုံးရပါမယ်။

----- BEGIN PRIVATE KEY BLOCK -----

----- END PRIVATE KEY BLOCK -----

သင့်ရဲ့ ကိုယ်ပိုင်စကားဝှက်သော့ကတော့ သင့်ဆီပို့လိုက်တဲ့ ကုဒ်ဖြင့်ပြောင်းလဲထားတဲ့ မက်ဆေ့ချ်တွေကို ပြန်ဖြည်ဖို့ သုံးနိုင်ပါတယ်။ ကုဒ်နဲ့ပြောင်းလဲထားတဲ့ မက်ဆေ့ချ်တွေကို ပြန်ဖြည်ဖို့သုံးတာဖြစ်လို့ သင့်ရဲ့ ကိုယ်ပိုင်စကားဝှက်သော့ကို လုံခြုံတဲ့နေရာမှာသိမ်းဆည်းထားဖို့လိုပါတယ်။ ဒါ့အပြင် သင့်ဆီက ပို့တဲ့စာရွက်စာတမ်းတွေမှာ သင်အစစ်အမှန် ဖြစ်ကြောင်း အတည်ပြုလို့ရတဲ့ ဒစ်ဂျစ်တယ် လက်မှတ်အဖြစ်လည်း ကိုယ်ပိုင်စကားဝှက်သော့ကို အသုံးပြုနိုင်ပါတယ်။

ကိုယ်ပိုင်စကားဝှက်သော့ဆိုတာ သင့်စက်ပစ္စည်းထဲမှာသိမ်းထားရမယ့် ဖိုင်တစ်ခုသာဖြစ်တာမို့ သင့်အနေနဲ့ ကိုယ်ပိုင်စကားဝှက်သော့သိမ်းထားတဲ့စက်ကို ကုဒ်နဲ့ပြောင်းလဲထားဖို့နဲ့ ခိုင်မာတဲ့ စကားဝှက်သုံးပြီးသိမ်းဖို့ အကြံပြုပါတယ်။ Surveillance Self-Defense မှာ ခိုင်မာသောစကားဝှက်များ ဖန်တီးခြင်းနဲ့ စက်ပစ္စည်းများကို ကုဒ်ဖြင့်ပြောင်းလဲခြင်း တို့အတွက် လမ်းညွှန်တွေ တင်ထားပေးပါတယ်။

public

private

----- BEGIN PUBLIC KEY BLOCK -----

----- BEGIN PRIVATE KEY BLOCK -----

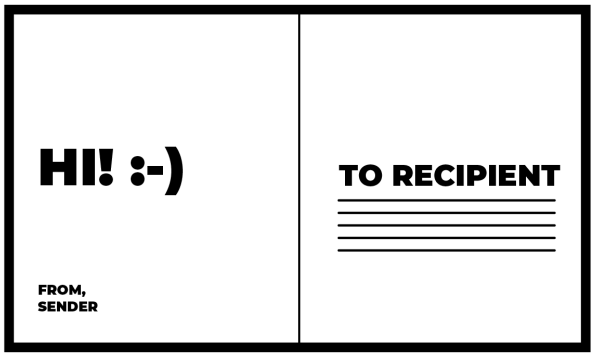
----- END PUBLIC KEY BLOCK -----

----- END PRIVATE KEY BLOCK -----

အများသုံးစကားဝှက်သော့	ကိုယ်ပိုင်စကားဝှက်သော့
• လူအများထံ ပေးထားလို့ရသည့်သော့ (အင်တာနက်မှ တဆင့် ပေးပို့မျှဝေနိုင်သည့်သော့)	• မိမိလက်ထဲတွင်သာ လုံခြုံစွာသိမ်းဆည်းရမည့်သော့
• ပေးပို့သူက မက်ဆေ့ချ်ကို ကုဒ်ဖြင့်ပြောင်းလဲဖို့ လက်ခံသူရဲ့ အများသုံးစကားဝှက်သော့ကို အသုံးပြုရ	• မိမိရဲ့ အများသုံးစကားဝှက်သော့ကို သုံးပြီးပေးပို့လာတဲ့ ကုဒ်နဲ့ ပြောင်းလဲထားသော မက်ဆေ့ ချ်ကို ပြန်ဖြည်ဖို့ သုံး

• အများသုံး စကားဝှက်သော့လက်ဗွေ ကိုသုံးပြီး မည်သူမည်ဝါဖြစ်ကြောင်း အတည်ပြုစစ်ဆေးနိုင်	• ဒီဂျစ်တယ်လက်ဗွေအဖြစ် သုံးပြီး ပေးပို့သူက မည်သူမည်ဝါဖြစ်ကြောင်း ကို အတည်ပြုစစ်ဆေးနိုင်
• လူအများဝင်ရောက်ကြည့်ရှုနိုင်သည့် ဒေတာဘေ့စ်များ ဥပမာ- “စကားဝှက်ဆာဗာများ” တွင် တင်ထားနိုင်သည်။ (PGP သုံး ကုဒ်ဖြင့်ပြောင်းလဲသည့် အီးမေလ်များတွင် စကားဝှက်ဆာဗာများကို တွင်ကျယ်စွာသုံးသည်	

“ရွေ့လျားဒေတာ” ကို ပို့စ်ကဒ်နဲ့စာပို့တာနဲ့ နှိုင်းယှဉ်စဉ်းစားလို့ရပါတယ်။ အောက်မှာဘယ်ဘက်ကပုံမှာ “ဟိုင်း”လို့ရေးထားတဲ့ပို့စ်ကဒ်ကို မြင်ရမှာပါ။ ပေးပို့သူက လက်ခံသူရဲ့လိပ်စာကိုရေးထားပါတယ်။ မက်ဆေ့ချ်ကို ကုဒ်နဲ့ပြောင်းလဲထားခြင်းမရှိလို့ ပို့စ်ကဒ်ကို တွေ့သူတိုင်းက ရေးထားတဲ့စာကို ဖတ်လို့ရပါတယ်။



ညာဘက်မှာတော့ တူညီတဲ့ပို့စ်ကဒ်မှာပဲ ကုဒ်နဲ့ပြောင်းလဲထားတဲ့ မက်ဆေ့ချ်ကိုရေးထားပါတယ်။ “ဟိုင်း” လို့ရေးတားပေမဲ့ ပေးပို့သူနဲ့လက်ခံသူ နှစ်ဦးကလွဲလို့ အခြားသူတွေဖတ်တဲ့အခါ ဖတ်မရတဲ့စာတွေ အဖြစ်မြင်ရပါတယ်။

ဒီလိုဖြစ်အောင် ဘယ်လိုလုပ်သလဲ။ ပေးပို့သူက လက်ခံသူရဲ့ အများသုံးစကားဝှက်သော့ကို ရရှိထားပါတယ်။ ပေးပို့သူက လက်ခံသူရဲ့ အများသုံးစကားဝှက်သော့ကိုသုံးပြီး မက်ဆေ့ခ်ကို ကုဒ်ပြောင်းလဲမှု

လုပ်ပါတယ်။ ဒါ့အပြင် ပေးပို့သူက သူ့ဆီက ပေးပို့တဲ့ မက်ဆေ့ချ်အစစ်အမှန်ဖြစ်ကြောင်း အတည်ပြုနိုင်ဖို့ ဒစ်ဂျစ်တယ်လက်မှတ်ကိုပါ ထည့်ပေးလိုက်ပါတယ်။

ဒီနေရာမှာ သတိပြုရမယ့်အချက်က အချက်အလက်တွေအကြောင်းရှင်းပြတဲ့ အချက်အလက်တွေ ဖြစ်တဲ့မက်ဆေ့ချ်ကို ဘယ်သူကဘယ်သူ့ဆီပို့တာ၊ ဘယ်အချိန်ကပို့တာ၊ ဘယ်အချိန်မှာလက်ခံရရှိတာ၊ ဘယ်နေရာတွေကို ဖြတ်စီးထားတယ်ဆိုတာတွေကိုတော့ မြင်နေရမှာပါ။ မက်ဆေ့ချ်မှာပါတဲ့ အကြောင်းအရာတွေကို မသိနိုင်ပေမဲ့ ဘယ်သူနဲ့ ဘယ်သူအကြားမှာ မက်ဆေ့ချ်တွေကို ကုဒ်နဲ့ပြောင်းလဲပြီး ပေးပို့နေတယ်ဆိုတာကိုတော့ သိရပါတယ်။

ဘယ်သူ့ဆီကို ကုဒ်နဲ့ပြောင်းလဲပြီးပို့တာလဲ။ လက်ခံသူကရော ကိုယ်ဆက်သွယ် လိုက်တဲ့သူဟုတ်ရဲ့လားဆိုတာကို ဘယ်လိုသိနိုင်မလဲ?

“ဟုတ်ပြီ၊ တစ်စုံတစ်ယောက်က ငါ့ရဲ့ အများသုံး စကားဝှက်သော့ ကိုသုံးပြီး ကုဒ်နဲ့ပြောင်းလဲထားတဲ့ မက်ဆေ့ချ်ကိုပို့မယ်၊ ငါ့က ကိုယ်ပိုင်စကားဝှက်သော့နဲ့ ပြန်ဖြည်မယ်။ ဒါပေမဲ့ တစ်ခြားသူတစ်ဦးက ငါလို့ ဟန်ဆောင်လိုက်ရင် ဘယ်လိုလုပ်မလဲ။ အဲဒီလူက အများသုံးစကားဝှက်သော့နှင့် ကိုယ်ပိုင် စကားဝှက်သော့အသစ်တစ်စုံဖန်တီးပြီး ငါ့နေရာမှာဟန်ဆောင်နေရင် ဘယ်လိုလုပ်မလဲ” ဆိုတဲ့ မေးခွန်းရှိလာနိုင်ပါတယ်။

အများသုံးစကားဝှက်သော့ပါ ဝှက်စာဗေဒ နည်းစနစ်က ဒီလိုပြဿနာတွေကို ရှောင်လွှဲဖို့ အလွန် အသုံးဝင်ပါတယ်။ ဒီနည်းစနစ်ကသင်ရော၊ လက်ခံသူနေရာနှစ်ဦးလုံးရဲ့ မှန်ကန်မှုကို အတည်ပြုပေးနိုင်ပါတယ်။ ကိုယ်ပိုင်စကားဝှက်သော့ရဲ့လုပ်ဆောင်ချက်တွေကို အသေးစိတ် လေ့လာကြည့်ရအောင်။

privkey.asc
id_rsa
private.der
private.pem

----- BEGIN PRIVATE KEY BLOCK -----

----- END PRIVATE KEY BLOCK -----

ကိုယ်ပိုင်စကားဝှက်သော့ရဲ့ လုပ်ဆောင်ချက်တွေထဲမှာ မိမိရဲ့ အများသုံးစကားဝှက်သော့ကိုသုံးပြီး ကုဒ်နဲ့ပြောင်းထားတဲ့ မက်ဆေ့ချ်တွေကို ပြန်ဖြည်တာအပြင် မိမိပို့တဲ့ မက်ဆေ့ချ်တွေထဲမှာ ဘယ်သူမှအတုလုပ်လို့မရတဲ့ ဒစ်ဂျစ်တယ် လက်မှတ်ထိုးပေးတာကိုလည်း လုပ်ပေးနိုင်ပါတယ်။ “အဲဒီလက်မှတ်ပါတဲ့မက်ဆေ့ချ်တိုင်းက ငါပို့တာ” လို့သေချာစေတဲ့ လက်မှတ်မျိုးပဲဖြစ်ပါတယ်။

သင့်မက်ဆေ့ချ်ကိုလက်ခံသူက သင့်ရဲ့ဒစ်ဂျစ်တယ်လက်မှတ်ကိုတွေ့ရင် သင့်အများသုံးစကားဝှက်သော့မှာပါတဲ့ အချက်အလက်တွေနဲ့ တိုက်ဆိုင်စစ်ဆေးလို့ရပါတယ်။

လက်တွေ့မှာ ဘယ်လိုအလုပ်လုပ်သလဲ ကြည့်ရအောင်။

မည်သူမည်ဝါစစ်မှန်ကြောင်း အတည်ပြုစစ်ဆေးခြင်း- အများသုံးစကားဝှက်သော့လက်မှေများ

ကျွန်ုပ်တို့ မက်ဆေ့ချ်တွေပို့တဲ့အခါ လမ်းမှာ အဆင့်ဆင့် ကြားပါဝင်သူတွေအနေနဲ့ မှန်ကန်တဲ့ လုပ်ရပ်တွေကို လုပ်ဖို့မျှော်လင့်ပါတယ်။ ဆိုလိုတာက ကျွန်ုပ်တို့ စာပို့တဲ့အခါ စာပို့သမားက စာကို ဖောက်ကြည့်တာ၊ စာကိုပြင်ပြီးမှပို့တာ မျိုးမလုပ်ဖို့ မျှော်လင့်သလိုပါပဲ။ ဒီအခြေအနေမျိုး ဖြစ်မလာနိုင်ဘူးလားဆို တော့လည်း စွန့်စားရတဲ့ အခြေအနေ ရှိနေပြန်ရော။

ကုဒ်နဲ့ပြောင်းလဲထားတဲ့ မက်ဆေ့ချ်တွေကိုလည်း ခိုးယူတာ၊ ပြောင်းလဲတာမျိုးလုပ်နိုင်တာမို့ အများသုံးစကားဝှက်သော့က ဒီဂျစ်တယ်စနစ်ကပေးပို့သူဟာ အပြင်ကပေးပို့သူနဲ့ တစ်ယောက်တည်းလား ဆိုတာကို တိုက်ဆိုင်စစ်ဆေးနိုင်ဖို့ ကူညီပေးပါတယ်။

အများသုံးစကားဝှက်သော့ဆိုတာ စာတွေအများကြီးရေးထားတဲ့ ဖိုင်တစ်ခုပဲ ဖြစ်ပါတယ်။ သူနဲ့ချိတ်ထားတာကတော့ ဖတ်လို့ရတဲ့ စကားဝှက်လက်မှေ ပါ။

ကွန်ပျူတာ လုံခြုံရေးနယ်ပယ်မှာ လက်မှေ ဆိုတဲ့စကားအတွက် အဓိပ္ပါယ်အမျိုးမျိုး ရှိပါတယ်။

“သော့စကားဝှက်” ဆိုတဲ့ အသုံးအနှုံးမှာဆိုရင် “65834 02604 86283 29728 37069 98932 73120 14774 81777 73663 16574 23234” လိုမျိုး ကိန်းဂဏန်းအရှည်ကြီးပါဝင်ပါတယ်။ အဲဒါကို အသုံးပြုပြီး လူတစ်ယောက်က မှန်ကန်တဲ့ ကိုယ်ပိုင်စကားဝှက်သော့ကို သုံးလား၊ မသုံးဖူးလားဆိုတာကို လုံလုံခြုံခြုံ အတည်ပြုစစ်ဆေးလို့ရပါတယ်။

အချို့ အက်ပ်တွေမှာဆိုရင် ဒီအချက်အလက်တွေကို QR code အနေနဲ့ မြင်တွေ့ရပြီး သင်နဲ့ သင့်မိတ်ဆွေအကြား အဲဒီ QR code တွေကို အပြန်အလှန်စကန်ဖတ်ပြီး အတည်ပြုနိုင်ပါတယ်။

“လက်ဗွေအတည်ပြုခြင်း” နည်းလမ်းနဲ့လည်း လူတစ်ယောက်ရဲ့ ဒစ်ဂျစ်တယ်မှတ်ပုံတင် မှန်ကန်မှုရှိ၊ မရှိဆိုတာ စစ်ဆေးလို့ရပါတယ်။

လက်ဗွေအတည်ပြုခြင်းကို အပြင်မှာလုပ်နိုင်ရင်တော့ အကောင်းဆုံးပါပဲ။ သင်နဲ့သင့်မိတ်ဆွေတို့ လူချင်းတနေရာမှာတွေ့ပြီး သူ့ဆီမှာရှိတဲ့ သင့်ရဲ့အများသုံးစကားဝှက်သော့နဲ့ သင့်ရဲ့သော့တို့ တူညီမှုရှိမရှိကို အက္ခရာတစ်ခုချင်း တိုက်ဆိုင်စစ်ဆေးသင့်ပါတယ်။ “342e 2309 bd20 0912 ff10 6c63 2192 1928” လို အက္ခရာစဉ်ကို တိုက်စစ်နေရတာ လက်ဝင်ပေမဲ့ လုံခြုံရေးအတွက် လုပ်ထားသင့်ပါတယ်။ တကယ်လို့လူချင်းမတွေ့နိုင်ရင်တော့ အစ-အဆုံးကုဒ်ဖြင့် ပြောင်းလဲခြင်းကို သုံးတဲ့ မက်ဆေ့ချ်စနစ် (သို့မဟုတ်) ချက်တင်စနစ်ကတဆင့် ပို့တာမျိုး (သို့မဟုတ်) HTTPS ဆိုက်မှာ ပို့စ်တင်တာမျိုးလို လုံခြုံတဲ့ လမ်းကြောင်းနဲ့ သင့်လက်ဗွေကို ပို့သင့်ပါတယ်။

စကားဝှက်သော့လက်ဗွေနဲ့ အတည်ပြုခြင်းကို လုပ်နိုင်လေလေ ကိုယ့်ဆီပို့တဲ့သူက ကိုယ်တကယ် ဆက်သွယ်လိုတဲ့သူဖြစ်ဖို့ ပိုသေချာလေလေပါပဲ။ ရာနှုန်းပြည့်တော့ မဟုတ်ဘူးပေါ့။ ကိုယ့်ရဲ့ ကိုယ်ပိုင်

စကားဝှက်သော့ကို ပုံတူပွားခြင်း (သို့မဟုတ်) ခိုးယူခြင်း (သင့်စက်ပစ္စည်းကို မောလ်ဝဲလ်ထည့်ပြီး တိုက်ခိုက်တာ/ သင့်စက်ပစ္စည်းထဲကို ကိုယ်ထိလက်ရောက်ဝင်ရောက်ပြီးဖိုင်ကို မိတ္တူပွားတာ) ခံရတဲ့အခါမျိုးမှာတော့ တစ်စုံတစ်ယောက်က သင့်အယောင်ဆောင်နိုင်တယ်လေ။ ဒါ့ကြောင့် သင့်ရဲ့ ကိုယ်ပိုင်စကားဝှက်သော့ခိုးယူခြင်းခံရတဲ့အခါမျိုးမှာ အဟောင်းကို မသုံးတော့ပဲ အများသုံးနဲ့ ကိုယ်ပိုင်စကားဝှက် သော့အသစ်တစ်စုံ ထပ်ပြီး ဖန်တီးဖို့လိုပါတယ်။ အများသုံးစကားဝှက် သော့အသစ်ကိုတော့ မိတ်ဆွေတွေဆီမျှဝေထားဖို့ လိုပါလိမ့်မယ်။

အကျဉ်းချုပ် - အများသုံးစကားဝှက်သော့ဖြင့် ကုဒ်ပြောင်းလဲခြင်း၏ လုပ်ဆောင်ချက်များ

အများသုံးစကားဝှက်သော့ဖြင့် ကုဒ်ပြောင်းလဲခြင်းက အသုံးပြုသူများအတွက် အောက်မှာ ဖော်ပြထားတဲ့ လုပ်ဆောင်ချက်တွေကို ပံပိုးပေးနိုင်ပါတယ်။

လျှို့ဝှက်မှု - အများသုံး စကားဝှက်သော့ ဖြင့် ကုဒ်ပြောင်းလဲခြင်းလုပ်ထားခြင်းအားဖြင့် လျှို့ဝှက်မက်ဆေ့ချ်တွေကို ဖန်တီးနိုင်ပြီး ရည်မှန်းထားတဲ့ လက်ခံသူကသာ ဖတ်လို့ရမှာဖြစ်ပါတယ်။

စစ်မှန်မှု - အများသုံးစကားဝှက်သော့ဖြင့် ကုဒ်ပြောင်းလဲခြင်း လုပ်ထားခြင်းအားဖြင့် ပေးပို့သူရဲ့ အများသုံးစကားဝှက်သာ သင့်လက်ထဲရှိနေမယ်ဆိုရင် ပေးပို့သူ တစ်ယောက်တည်းကပဲ မက်ဆေ့ချ်ကို ရေးတယ်ဆိုတဲ့ စစ်မှန်မှုကို အတည်ပြုလို့ရပါမယ်။

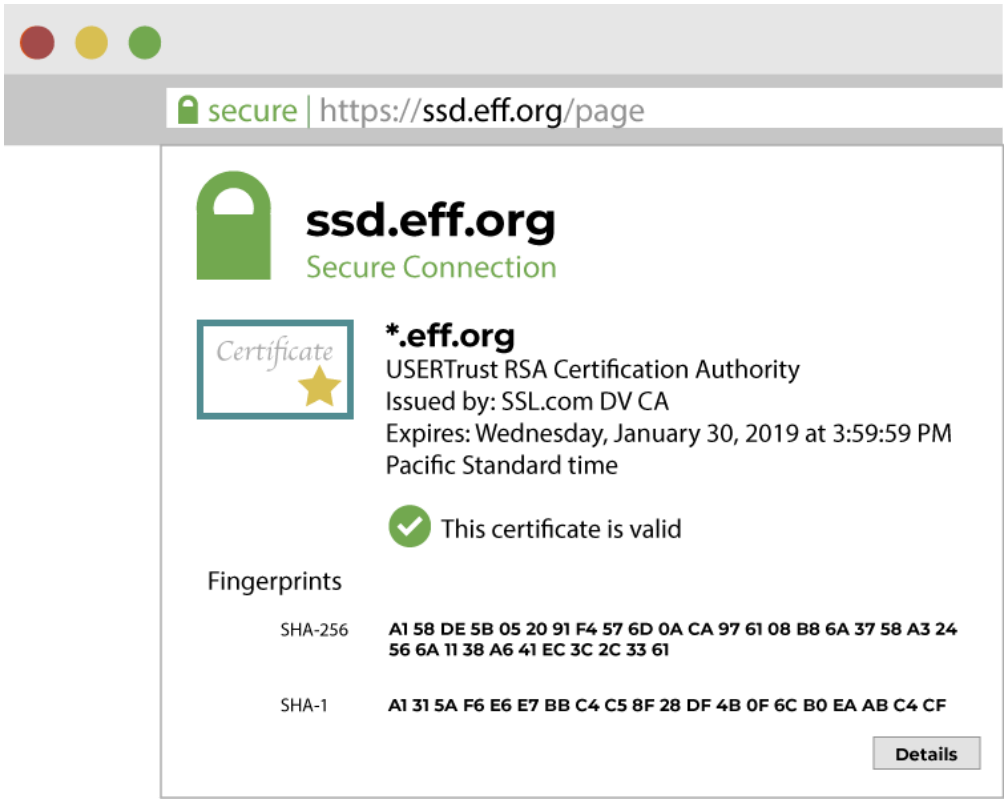
အတုအပကင်းစင်မှု - လက်မှတ်ထိုးထားတဲ့ မက်ဆေချ် (သို့မဟုတ်) အများသုံးစကားဝှက်သော့ ဖြင့်ကုဒ်ပြောင်းလဲထားတဲ့ မက်ဆေ့ချ်တွေဟာ များသောအားဖြင့် အတုလုပ်လို့ မရပါဘူး။ အတုဆိုရင် ပြန်ဖြည် လို့ရမှာမဟုတ်ပါဘူး။ ဆိုလိုတာက ပေးပို့လိုက်တဲ့ မက်ဆေ့ချ်ကို ပြုပြင်ပြောင်းလဲထားတာမျိုးနဲ့ မရည်ရွယ်တဲ့ အပြောင်းအလဲမျိုးရှိနေခဲ့ရင်တောင် (ယာယီနက်ဝေါ့ခ်ပြဿနာကြောင့်) ချက်ချင်း သိနိုင်ပါတယ်။

ဝက်ဘ်ဆိုက်များနှင့် ဝန်ဆောင်မှုများ၏ မှန်ကန်မှုကို အတည်ပြုခြင်း- လုံခြုံရေးအသိအမှတ်ပြုကုဒ်များ

သင့်အနေနဲ့ “အများသုံးစကားဝှက်သော့လက်ဗွေနဲ့ လူကိုအတည်ပြုစစ်ဆေးတာကိုတော့ လုပ်နိုင်ပြီ။ ဒါဆိုရင် ဝက်ဘ်ဆိုက်တွေရဲ့ မှန်ကန်မှုကိုရော ဘယ်လိုစစ်ဆေးမလဲ။ ကိုယ်ဝင်ရောက်တဲ့ ဝက်ဘ်ဆိုက် (သို့မဟုတ်) ရယူတဲ့ဝန်ဆောင်မှုဟာ အစစ်ဟုတ်၊ မဟုတ် ဘယ်လိုစစ်ဆေးမလဲ။ ကြားထဲမှာ အနှောင့်အယှက်တွေရှိ၊ မရှိဘယ်လိုသိနိုင်မလဲ” ဆိုတဲ့ မေးခွန်းမျိုး ရှိနေနိုင်ပါတယ်။

အစ-အဆုံးကုဒ်ဖြင့်ပြောင်းလဲခြင်းကို သုံးတဲ့သူတွေက သူတို့ရဲ့ အများသုံးစကားဝှက်သော့တွေကို လူအများဆီပေးထားလိုက်ရင် မက်ဆေ့ချ်ပို့သူဟာ သော့ပိုင်ရှင် အစစ်အမှန်ဖြစ်ကြောင်းကို အတည်ပြုလို့ရမယ်။ ထိုနည်းတူပဲ သင့်ကွန်ပျူတာမှာ သယ်ယူပို့ဆောင်ရေးအလွှာတွင် ကုဒ်ဖြင့်ပြောင်းလဲခြင်းကို သုံးထားမယ်ဆိုရင် သင်ဝင်တဲ့ဆိုက်မှာရှိတဲ့ အများသုံးစကားဝှက်သော့နဲ့ ဝန်ဆောင်မှု အစစ်အမှန်ရဲ့ အများသုံးစကားဝှက်သော့တွေကို တိုက်ဆိုင်စစ်ဆေးပြီး အတည်ပြုပေးပါတယ်။ အဲဒါကို လုံခြုံရေး အသိအမှတ်ပြုကုဒ် လို့ခေါ်ပါတယ်။

အောက်ကပုံမှာတော့ ဝက်ဘ်ဘရောင်ဇာ တစ်ခုရဲ့ SSD အတွက် လုံခြုံရေး အသိအမှတ်ပြုကုဒ် ကို ဥပမာပြထားပါတယ်။ လုံခြုံရေးဆိုင်ရာအချက်အလက်တွေကို များသောအားဖြင့် သင့်ရဲ့ ဝက်ဘ်ဘရောင်ဇာမှာပါတဲ့ HTTPS သော့ခလောက်ပုံလေး ကိုနှိပ်ပြီးရယူနိုင်ပါတယ်။



သင့်ဝက်ဘ်ဘရောက်ဇာက HTTPS ကို သုံးပြီး ကုဒ်နဲ့ပြောင်းလဲထားတဲ့ချိတ်ဆက်မှုတွေကို လုပ်နိုင်ပါတယ်။ ဆိုက်အစစ် အမှန်တွေနဲ့ လုံခြုံတဲ့ချိတ်ဆက်မှုရှိကြောင်း သက်သေပြဖို့အတွက် ဝက်ဘ်ဆိုဒ်တွေက လုံခြုံရေးအသိအမှတ်ပြုကုဒ်ကို သုံးပါတယ်။ ဝက်ဘ်ဘရောက်ဇာတွေက ဆိုက်တွေရဲ့ လုံခြုံရေးအသိ အမှတ်ပြုကုဒ်ကို အများသုံးဝှက်စာသော့တွေကို ဖော်ပြတဲ့ ဒိုမိန်းတွေဖြစ်တဲ့

www.google.com, www.amazon.com, (သို့) ssd.eff.org စတဲ့ နေရာတွေမှာ သွားရောက်စစ်ဆေးပါတယ်။ ဒီလုံခြုံရေးအသိ အမှတ်ပြုကုဒ်တွေက လူတစ်ယောက် (သို့မဟုတ်)

ဝက်ဘ်ဆိုက်တစ်ခုရဲ့ အများသုံးစကားဝှက်သော့ မှန်/မမှန်ဆိုတာကို စစ်ဆေးတဲ့နည်းလမ်းတစ်ခုဖြစ်ပါတယ်။ ဒါပေမဲ့ သင်ဝင်ရောက်ကြည့်ရှုတဲ့ ဆိုက်ရဲ့ အများသုံးစကားဝှက်သော့အမှန်က ဘာလဲဆိုတာကို သင့်ကွန်ပျူတာက ဘယ်လိုရှာဖွေနိုင်မလဲ။

ခေတ်ပေါ်ဘရောက်ဇာတွေနဲ့ လည်ပတ်မှုစနစ်တွေမှာ ယုံကြည်ရတဲ့ လုံခြုံရေးအသိအမှတ်ပြုပေးသည့် အာဏာပိုင်များ (CAs) စာရင်း ပါရှိပါတယ်။ အဲဒီ CAs တွေရဲ့ အများပိုင်စကားဝှက်သော့တွေဟာ သင် ဘရောက်ဇာကိုဒေါင်းလုတ်ဆွဲချိန် (သို့မဟုတ်) ကွန်ပျူတာအသစ်ထဲမှာ အလိုအလျောက်ပါလာပြီးသား ဖြစ်ပါတယ်။ လုံခြုံရေးအသိအမှတ်ပြုပေးတဲ့ အာဏာပိုင်တွေက ဝက်ဘက်ဆိုက်တွေဟာ ခွင့်ပြုထားတဲ့ ဒိုမိန်း (ဥပမာ- www.example.com) နဲ့ တရားဝင်လည်ပတ်နေတယ်ဆိုတာကို အသိအမှတ်ပြုပြီးရင် ဆိုင်ရာဝက်ဘ်ဆိုက်တွေရဲ့ အများသုံးစကားဝှက်သော့မှာ အာဏာပိုင်တွေက လက်မှတ်ထိုးပေးပါတယ်။ သင့်အနေနဲ့ HTTPS ဆိုက်ထဲဝင်တဲ့အခါ သင့်ဘရောက်ဇာက အဲဒီဆိုက်မှာ CA လက်မှတ်ပါ/မပါ အတည်ပြုပေးပါတယ်။ ဆိုလိုတာက သင်ဝင်ရောက်တဲ့ ဝက်ဘက်ဆိုက်က အစစ်အမှန်ဖြစ်ကြောင်း တတိယပါတီရဲ့ အတည်ပြုချက်ရှိတယ်လို့ ဆိုတာပါပဲ။

ဒါပေမဲ့တစ်ခုရှိတာက လုံခြုံရေးအသိအမှတ်ပြုကုဒ်မှာ CA ရဲ့ လက်မှတ်ပါတိုင်း အဲဒီဆိုက်က လုံခြုံတယ်လို့တော့ အာမခံချက်မရှိပါဘူး။ CA ကိုသုံးပြီး အတည်ပြုတာလည်း အကန့်အသတ်ရှိပါတယ်။ အသိအမှတ်ပြုလက်မှတ်ရထားတဲ့ ဝက်ဘက်ဆိုက်တိုင်းကို ရိုးသားပြီး ယုံကြည်လို့ရတဲ့ ဆိုက်တွေလို့ သတ်မှတ်လို့မရပါဘူး။ ဥပမာ- ဝက်ဘ်ဆိုက်တစ်ခုက HTTPS ကို သုံးထားသည့်တိုင် လိမ်ဆင်တွေ (သို့) malware တွေကို လက်ခံထားနိုင်ပါသေးတယ်။ ပိုပြီး အသေးစိတ်သိနိုင်ဖို့ ကျွန်ုပ်တို့ရေးသား ထားတဲ့ မောလ်ဝဲလ်နဲ့ ဖစ်ရှင်းအကြောင်း လမ်းညွှန်ကိုဖတ်ပါ။

သင့်အနေနဲ့ ဒီအသိအမှတ်ပြုလက်မှတ်တွေနဲ့ပတ်သက်လို့ အမှားအယွင်းဖြစ်နေကြောင်း မက်ဆေ့ချ်တွေ မကြာခဏမြင်ရပါလိမ့်မယ်။ များသောအားဖြင့်တော့ ဒါဟာ စနစ်ရဲ့အမှား ဖြစ်တတ်ပါတယ်။ သင့်ချိတ်ဆက်ထားတဲ့ ဟိုတယ် (သို့) ကော်ဖီဆိုင်ရဲ့နက်ဝေါ့ခ်က ဆိုက်ကိုမချိတ်ခင်မှာ သူတို့ရဲ့ ဤ အဝင်စာမျက်နှာကို ချိတ်ဖို့ကြိုးစားလို့ဖြစ်ပါတယ်။ တခါတရံမှာတော့ ဟက်ကာ (သို့) သူခိုး (သို့) ရဲ (သို့) ထောက်လှမ်းရေး အေဂျင်စီတွေက သင့်ရဲ့ ကုဒ်နဲ့ပြောင်းလဲထားတဲ့ ချိတ်ဆက်မှုကို ဖျက်ဆီးဖို့ ကြိုးစားရင်လည်း ဒီလို မက်ဆေ့ချ်တွေရတတ်ပါတယ်။ စနစ်အမှားလား သင့်ကို ဟက်ခ်တာလား ဆိုတာကိုတော့ ခွဲခြားဖို့ ခက်ပါတယ်။

ဆိုလိုတာက သင့်အနေနဲ့ သတိပေးစာမြင်ရရင် လျစ်လျူမရှုဖို့ပါပဲ။ အထူးသဖြင့် အဲဒီဆိုက်က သင့်ရဲ့ အရေးကြီးတဲ့ အချက်အလက်တွေ (သို့) အကောင့်ရှိနေရင်ပေါ့။

ဘက်ညီစကားဝှက်သော့များ၊ ဘက်မညီစကားဝှက်သော့များနှင့် အများသုံးစကားဝှက်သော့လက်ဗွေများအကြောင်း အချုပ်

သယ်ယူပို့ဆောင်ရေးအလွှာ၏ လုံခြုံရေးလက်ဆွဲနှုတ်ဆက်မှုဆိုင်ရာ ဥပမာ

ဒေတာ သယ်ယူပို့ဆောင်ရေးအလွှာတွင် ကုဒ်ဖြင့်ပြောင်းလဲခြင်းနည်းစနစ်ကို အသုံးပြုတဲ့အခါ သင့် ဘရောက်ဇာနဲ့ သင်ဝင်ရောက်ကြည့်ရှုတဲ့ ဝက်ဘ်ဆိုက်ရဲ့ ကွန်ပျူတာတွေက ဘက်ညီ အယ်လ်ဂိုရစ်သမ်ရော၊ ဘက်မညီ အယ်လ်ဂိုရစ်သမ်နှစ်မျိုးလုံးကို သုံးပါတယ်။

ဒီနှစ်မျိုးလုံး ဘယ်လိုအလုပ်လုပ်သလဲဆိုတာ ဆန်းစစ်ကြည့်ရအောင်။ HTTPS ဝက်ဘ်ဆိုက် (https://ssd.eff.org/) ကို သင်ချိတ်ဆက်လိုက်တဲ့အခါ ဘာတွေဆက်ဖြစ်သလဲ။

ဝက်ဘ်ဆိုက်က HTTPS ကို သုံးတဲ့အခါ၊ သင့်ဘရောက်ဇာနဲ့ ဝက်ဘ်ဆိုက်ဆာဗာအကြားမှာ အလွန်မြန်ဆန်တဲ့ ထိတွေ့မှုတွေ ဖြစ်ပါတယ်။ အဲဒါကို လက်ဆွဲနှုတ်ဆက်တယ်လို့ တင်စားကြတာပါ။ သင့် ဘရောက်ဇာ (ဥပမာ- Google Chrome, Mozilla Firefox, Tor Browser) စတာတွေက ဝက်ဘ်ဆိုက် ဖြစ်တဲ့ https://ssd.eff.org. ထိုင်ထားတဲ့ ကွန်ပျူတာဆာဗာနဲ့ စကားပြောပါတယ်။

အဲဒီလက်ဆွဲနှုတ်ဆက်မှုမှာ ဘရောက်ဇာနဲ့ ဆာဗာတွေ အပြန်အလှန်စာတွေပို့ကြပြီး နှစ်ဖက်စလုံးက အသုံးပြုတဲ့ ကုဒ်ပြောင်းလဲခြင်းဆိုင်ရာ အယ်လ်ဂိုရစ်သမ်များ (cipher suites) ရှိ/မရှိ စစ်ဆေးကြပါတယ်။ ပြန်ရှင်းရရင် သင့်ဘရောက်ဇာနဲ့ ဆာဗာတွေက စကားပြောကြတာပေါ့။ ဘာပြောလဲဆိုတော့ ကုဒ်နဲ့ပြောင်းလဲခြင်းနည်းလမ်းတွေထဲက ဘယ်နည်းလမ်းကို သုံးသလဲ၊ ဘယ်ဟာကိုရွေးချယ်မလဲ ဆိုတာကို အပြန်အလှန်ပြောကြတယ်လို့ အလွယ်မှတ်နိုင်ပါတယ်။ သူတို့အပြန်အလှန်ပြောတာကို ဥပမာ ကြည့်ရအောင်။ (ငါတို့နှစ်ယောက်လုံး ဘက်မညီ အယ်လ်ဂိုရစ်သမ်ဖြစ်တဲ့ RSA နဲ့ ဘက်ညီ အယ်လ်ဂိုရစ်သမ်ဖြစ်တဲ့ AES တို့ ပေါင်းထားတဲ့ နည်းလမ်းကိုသိလား။ အင်းသိတယ်ဆိုရင်ကောင်းတာပေါ့။ ဒါပေမဲ့ အလုပ်မဖြစ်ဘူးဆိုရင် ဘယ် အယ်လ်ဂိုရစ်သမ်ကိုသုံးပြီး ကုဒ်ပြောင်းလဲမှုလုပ်ကြမလဲ) ဆိုတာမျိုးပြောကြတာပါ။

အဲဒီလို အပြန်အလှန်ဆက်သွယ်ပြီးရင်တော့ သင့်ဘရောက်ဇာက နှစ်ဖက်သဘောတူတဲ့ ဘက်မညီ ကုဒ်ပြောင်းလဲခြင်းနည်းလမ်းကို သုံးပြီး အများသုံးစကားဝှက်သော့လက်မှတ်ကို ssd.eff.org ကို ပို့ပြီး သင်ဟာ ဆက်သွယ်သူအစစ်အမှန်ဖြစ်ကြောင်း သက်သေခံပါလိမ့်မယ်။ ဆိုက်မှာရှိတဲ့ ဆာဗာတွေက သင့်ရဲ့ အများသုံးစကားဝှက်သော့နဲ့ ခုနကပို့ထားတဲ့ အများသုံးစကားဝှက်သော့လက်မှတ်တို့ကို တိုက်ဆိုင်စစ်ဆေးပြီး မှန်ကန်ကြောင်း အတည်ပြုပါလိမ့်မယ်။ ဒီလိုလုပ်တာက အခြားကွန်ပျူတာ တစ်ခုက သင့်ချိတ်ဆက်မှုကို အနှောင့်အယှက်ပြု ထောက်လှမ်းလို့မရအောင် လုပ်တာဖြစ်ပါတယ်။

သင့်ဟာ အသုံးပြုသူအစစ်အမှန်ဖြစ်ကြောင်း အတည်ပြုပြီးတာနဲ့ ဆိုက်ရဲ့ဆာဗာတွေက ဘက်ညီကုဒ် ဖြင့်ပြောင်းလဲခြင်းနည်းလမ်းကို သုံးပြီး ဘက်ညီတဲ့ လျှို့ဝှက်စကားဝှက်သော့ဖိုင်အသစ်ကို

ထုတ်ပေးပါလိမ့်မယ်။ အဲဒီသော့က သင့်ဘရောက်ဇာရဲ့ စကားဝှက်သော့ကို ဘက်မညီ ကုဒ်ပြောင်းလဲမှု လုပ်ပေးပြီး သင့်ဘရောက်ဇာဆီ ပို့လိုက်ပါတယ်။ သင့်ဘရောက်ဇာက သူ့ရဲ့ ကိုယ်ပိုင်စကားဝှက်သော့နဲ့ ပြန်ဖြည်ပါလိမ့်မယ်။

တကယ်လို့ ဘက်ညီစကားဝှက်သော့က အလုပ်ဖြစ်တယ်ဆိုရင် သင့်ဘရောက်ဇာနဲ့ ဝက်ဘက်ဆိုက် ဆာဗာက အဲဒီသော့ကိုသုံးပြီး ဆက်သွယ်မှုတိုင်းကို ကုဒ်နဲ့ပြောင်းလဲ ပေးမှာဖြစ်ပါတယ်။ (ဒီလို အပြန်အလှန်ဆက်သွယ်မှုတွေလုပ်တာကို သယ်ယူပို့ဆောင်ရေးအလွှာ လုံခြုံရေး (TLS) လက်ဆွဲနှုတ်ဆက်မှု) လို့ခေါ်ပါတယ်။) အားလုံးအဆင်ပြေသွားရင်၊ ssd.eff.org ကို သင့်ရဲ့ HTTPS ချိတ်ဆက်မှုက လုံခြုံသွားပါပြီ။ အများသုံးစကားဝှက်သော့နဲ့ ကိုယ်ပိုင်စကားဝှက်သော့တွေအကြောင်း၊ အတည်ပြုသက်သေခံခြင်း အကြောင်းတွေကို ပိုပြီးအသေးစိတ်သိချင်ရင်တော့ အများသုံးကုဒ်နဲ့ပြောင်းလဲခြင်းသော့ အကြောင်းလမ်းညွှန်မှာ ဖတ်ရှုနိုင်ပါတယ်။