EFF'S SURVEILLANCE SELF-DEFENSE

နှစ်ဆနေခံလုံခြုံရေးစနစ်ကို ဘယ်လို ဖွဲ့ရမလဲ

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

LOCALIZATION LAB

https://ssd.eff.org/en/module/how-enable-two-factor-authentication
Last reviewed:
2017-09-07

နှစ်ဆင့်ခံလုံခြုံရေးစနစ်ကို ဘယ်လို ဖွင့်ရမလဲ

နှစ်ဆင့်ခံလုံခြုံရေးစနစ် (သို့မဟုတ် 2FA) ဆိုတာကတော့ အသုံးပြုသူကနေပြီး ဝန်ဆောင်မှုတစ်ခုကို သုံးတဲ့အခါ မိမိကိုယ်ကို အတည်ပြုဖို့အတွက် မတူညီတဲ့ အဆင့်နှစ်ဆင့်ပေါင်းပြီး အတည်ပြုရတဲ့ နည်းလမ်းကို ဆိုလိုပါတယ်။ စနစ်က

- အသုံးပြုသူသိတဲ့ စကားဝှက် ဒါမှမဟုတ် PIN လိုမျိုးလည်း ဖြစ်နိုင်ပြီး
- အသုံးပြုသူပိုင်ဆိုင်တဲ့ ဖုန်းလိုမျိုးလည်း ဖြစ်နိုင်သလို
- အသုံးပြုသူနဲ့ ခွဲလို့ မရနိုင်တဲ့ လက်ဗွေရာလိုမျိုးလည်း ဖြစ်နိုင်ပါတယ်။

2FA ကို သင့်ဘဝမှာ တစ်ခုခုအတွက်တော့ အသုံးပြုပြီးသား ဖြစ်ချင်ဖြစ်နိုင်ပါတယ်။ ATM ကနေ ပိုက်ဆံထုတ်ချင်တဲ့အခါ အသုံးပြုသူပိုင်ဆိုင်တဲ့ ဘဏ်ကတ်ကိုလည်း ရှိဖို့လိုသလို အသုံးပြုသူသိတဲ့ PIN ကိုလည်း မှတ်မိဖို့ လိုတယ်လေ။ အခုလောလောဆယ်မှာတော့ အွန်လိုင်းဝန်ဆောင်မှုတော်တော်များများက အတည်ပြုဖို့အတွက် တစ်ခုတည်းဖြစ်တဲ့ စကားဝှက်ကို သုံးပြီး မိမိကိုယ်ကို အတည်ပြုလို့ပဲ ရပါတယ်။

2FA က အွန်လိုင်းမှာ ဘယ်လို အလုပ်လုပ်လဲ?

Facebook၊ Google နဲ့ Twitter တို့ အပါအဝင် အွန်လိုင်းဝန်ဆောင်မှု တော်တော်များများက စကားဝှက်ရဲ့ တခြားရွေးချယ်စရာအနေနဲ့ 2FA ကို သုံးပြီး အတည်ပြုလို့ရအောင် လုပ်ထားပါတယ်။ 2FA ကို ဖွင့်ထားလိုက်မယ်ဆိုရင် အကောင့်ကို ဝင်တဲ့အခါ စကားဝှက်နဲ့ရော နောက်ထပ်အတည်ပြုတဲ့ နည်းလမ်းတစ်ခုနဲ့ရော ဝင်ရမှာ ဖြစ်ပါတယ်။ နောက်ထပ်အတည်ပြုတဲ့နည်းလမ်းက SMS နဲ့ လက်ခံရရှိမယ့် တစ်ခါသုံးကုတ်လည်း ဖြစ်နိုင်သလို Google Authenticator၊ Duo Mobile၊ Facebook app၊ နဲ့ Clef စတဲ့ အတည်ပြုကုတ်ကို သက်သက်ထုတ်ပေးတဲ့ အပလီကေးရှင်းတွေက တစ်ခါသုံးကုတ်တွေလည်း ဖြစ်နိုင်ပါတယ်။ ဘယ်နည်းလမ်းပဲဖြစ်ဖြစ် သင်ပိုင်တဲ့ သင့်ဖုန်းရှိဖို့ကတော့ အရေးကြီးပါတယ်။ Google အပါအဝင် တစ်ချို့ဝဘ်ဆိုဒ်တွေမှာ တစ်ခါသုံး အရန်အတည်ပြုကုတ်တွေကို ထုတ်ပေးပါတယ်။ အဲဒီ့အရန်ကုတ်တွေကို ဒေါင်းလုတ်လုပ်ထားတာ၊ စာရွက်နဲ့ ပရင့်ထုတ်တာမျိုး လုပ်ထားပြီး အလုံခြုံဆုံး နေရာတစ်ခုခုမှာ သိမ်းထားလို့လည်း ရပါတယ်။ 2FA ကို စသုံးလိုက်ပြီဆိုတာနဲ့ အကောင့်ကို ဝင်တဲ့အခါမှာ စကားဝှက်အပြင် နောက်ထပ် တစ်ခါသုံးကုတ်ကိုလည်း ထည့်ပြီး ဝင်ရမှာ ဖြစ်ပါတယ်။

ဘာလို့ 2FA ကို သုံးသင့်တာလဲ?

2FA က သင့်အကောင့်ကို ဝင်ဖို့အတွက် အတည်ပြုတဲ့နေရာမှာ နည်းလမ်းတစ်ခုထက်ပိုပြီး လိုအပ်တဲ့အတွက် အကောင့်ရဲ့ လုံခြုံရေးကို ပိုအားကောင်းစေပါတယ်။ ဆိုလိုတာကတော့ တစ်ယောက်ယောက်က သင့်စကားဝှက်ကို သိနေတယ်ဆိုရင်တောင်မှ သင့်ဖုန်း ဒါမှမဟုတ် တစ်ခါသုံး အရန်အတည်ပြုကုတ် မရှိရင် အကောင့်ကို ဝင်လို့ မရပါဘူး။

2FA သုံးတဲ့အခါမှာ အားနည်းချက်တွေ ရှိလဲ?

2FA က ပိုပြီးလုံခြုံတဲ့ အတည်ပြုစနစ်ကို လုပ်ပေးပေမယ့်လည်း သင့်အတွက် ဆိုးကျိုးတွေ ရောက်လာနိုင်တာလည်း ဖြစ်နိုင်ပါတယ်။ ဥပမာ ဖုန်းကို နေရာအထားမှားတာ၊ ဖုန်းပျောက်သွားတာ၊ ဆင်းမ်ကတ် လဲလိုက်တာ၊ ဒါမှမဟုတ် တခြားနိုင်ငံတစ်ခုကို ခရီးသွားတဲ့အခါ roaming ကို မဖွင့်ထားတဲ့အခါမျိုးမှာ အကောင့် ဝင်လို့မရဖြစ်တတ်ပါတယ်။

2FA ဝန်ဆောင်မှုတော်တော်များများက တစ်ခါသုံး အရန်အတည်ပြုကုတ် (backup/ recovery code) တွေကို သုံးလို့ရအောင် လုပ်ပေးထားပါတယ်။ ကုတ်တစ်ခုက တစ်ခါဝင်ပြီးပြီဆိုရင် အဲဒီကုတ်နဲ့ နောက်တစ်ခါ ဝင်လို့ မရပါဘူး။ ဖုန်း ဒါမှမဟုတ် တခြားအတည်ပြုတဲ့ စက်ပစ္စည်း ပျောက်မှာစိုးရိမ်တယ်ဆိုရင် အတည်ပြုကုတ်တွေကို ပရင့်ထုတ်ပြီး သွားလေရာကို ယူသွားလို့ ရပါတယ်။ ဆိုတော့ အဲဒီကုတ်တွေက အသုံးပြုသူပိုင်ဆိုင်တဲ့အရာ အနေနဲ့ ဖြစ်နေမှာပေါ့။ ပရင့်ထုတ်ပြီး သိမ်းထားမယ်ဆိုရင် သတိထားဖို့လိုတာကတော့ ဘယ်သူကမှ ယူသွားလို့မရတဲ့ လုံလုံခြုံခြုံနေရာတစ်ခုမှာ သိမ်းထားတာ အကောင်းဆုံးပါပဲ။ ထုတ်ထားပြီးသား ကုတ်တွေ ပျောက်သွားတယ် ဒါမှမဟုတ် အကုန်လုံးကို သုံးပြီးသွားပြီဆိုရင် သင် ဝင်ထားပြီးသား အကောင့်ကနေ နောက်ထပ်ကုတ်တွေကို ထပ်ထုတ်ခိုင်းလို့ ရပါတယ်။

SMS နဲ့ ကုတ်ကို လက်ခံတဲ့ 2FA စနစ်ရဲ့ တခြားပြဿနာတစ်ခုကတော့ SMS စာပို့တဲ့ စနစ်က လုံခြုံမှု မရှိတာပါပဲ။ တယ်လီဖုန်းကွန်ယက်တွေနဲ့ လှမ်းချိတ်ပြီး အချက်အလက်တွေ ယူလို့ရနေတဲ့ နည်းပညာအားကောင်းတဲ့ တိုက်ခိုက်သူ/ အဖွဲ့အစည်းတွေက ကြားထဲကနေ SMS ကို ဖြတ်ယူပြီး ကုတ်နဲ့ ဝင်လို့ ရသွားတာမျိုးတွေ ဖြစ်နိုင်ပါတယ်။ နည်းပညာသိပ်အားမကောင်းတဲ့ တိုက်ခိုက်သူတွေက တခြားသူဆီ ဝင်လာတဲ့ ဖုန်းတွေကို သူတို့ဆီ ဝင်လာအောင် လုပ်တာမျိုး၊ ဖုန်းရှိစရာမလိုပဲ ဖုန်းနံပါတ်တစ်ခုကို စာပို့လိုက်တဲ့ ဝန်ဆောင်မှု ကုမ္ပဏီကို ကြားဖြတ်ယူတာမျိုးတွေလည်း ဖြစ်ခဲ့ဖူးတဲ့ ကိစ္စတွေ ရှိပါတယ်။

ဒီလိုမျိုး အခြေအနေရှိတဲ့ တိုက်ခိုက်မှုမျိုးကို စိတ်ပူတယ်ဆိုရင်တော့ SMS နဲ့ ကုတ်လက်ခံတာကို ပိတ်ထားလိုက်ပြီး Google Authenticator ဒါမှမဟုတ် Authy လိုမျိုး အပလီကေးရှင်းတွေကို သုံးလည်း ရပါတယ်။ ဒါပေမယ့် ကံမကောင်းစွာနဲ့ပဲ 2FA ပါတဲ့ ဝန်ဆောင်မှုတွေမှာ SMS နဲ့ ကုတ်လက်ခံတာကို ပိတ်ထားလို့ မရပါဘူး။

ထပ်လောင်းပြောရရင် 2FA သုံးတယ်ဆိုတာက ဝန်ဆောင်မှုတစ်ခုကို ကိုယ်ပေးချင်တဲ့ အချက်အလက်ထက် ပိုပြီး ပေးလိုက်ရတာမျိုးလည်း ဖြစ်နိုင်ပါတယ်။ ဆိုကြပါစို့ Twitter ကို နာမည်လွဲတစ်ခုနဲ့ သုံးတယ်။ Twitter ကို သုံးတဲ့အခါ သင့်ရဲ့ သတင်းအချက်အလက်တွေကို မရစေချင်တဲ့အတွက် Tor ဒါမှဟုတ် VPN တစ်ခုခုကို သုံးတယ်ဆိုရင်တောင်မှပဲ SMS နဲ့ 2FA ကုတ်ကို ရယူတဲ့ စနစ်ကို သုံးတယ်ဆိုရင် Twitter က သင့်ဖုန်းနံပါတ်ကို မှတ်ထားလို့ လိုအပ်လာပါတယ်။ အဓိပ္ပာယ်ကတော့ အကြောင်းတစ်စုံတစ်ရာကြောင့် လိုအပ်လာတယ်ဆိုရင် (ဥပမာ တရားရုံးကနေ တောင်းဆိုလာတယ်) ဆိုရင် Twitter က သင့်အကောင့်နဲ့ သင့်ဖုန်းနံပါတ်ကို ချိတ်ပေးလိုက်နိုင်ပါတယ်။ ဝန်ဆောင်မှုတစ်ခုပေါ်မှာ နာမည်အရင်းနဲ့ သုံးနေတဲ့လူဆိုရင်တော့ ပြဿနာမဟုတ်ပေမယ့် သင့်ရဲ့ အမည်မဖော်လိုမှုကို ကာကွယ်တာကလည်း အရေးကြီးပါတယ်။ ဒါကြောင့်မို့လို့ SMS နဲ့ 2FA ကုတ်ကို ရယူတဲ့ စနစ်ကို မသုံးခင် သေချာစဉ်းစားစေချင်ပါတယ်။

2FA သုံးပြီးတဲ့အခါ 2FA က လုံခြုံအောင် လုပ်ပေးမယ်ဆိုတဲ့ ခံယူချက်နဲ့ အသုံးပြုသူ တစ်ချို့က အားမကောင်းတဲ့ စကားဝှက်တွေ ပေးလာကြတယ်ဆိုတာကို သုတေသနတစ်ချို့ကလည်း သက်သေပြထားပါတယ်။ 2FA ကို သုံးနေတယ်ဆိုရင်တောင်မှပဲ အားကောင်းတဲ့ စကားဝှက်ထားဖို့ အရေးကြီးပါတယ်။ အားကောင်းတဲ့ စကားဝှက်ဖြစ်အောင် ဘယ်လိုထားရမယ်ဆိုတာကို ဒီမှာ ကြည့်လို့ရပါတယ်။

2FA ကို ဘယ်လို ဖွင့်ရမလဲ?

ဒါကတော့ ဝန်ဆောင်မှုတစ်ခုနဲ့ တစ်ခုက မတူပါဘူး။ 2FA သုံးလို့ရတဲ့ ဝန်ဆောင်မှုတွေ စာရင်းကို https://twofactorauth.org/ ဒီမှာလည်း ကြည့်လို့ရပါတယ်။ ဘယ်လို ဖွင့်ရမယ်ဆိုတာကိုတော့

သာမန်ဝန်ဆောင်မှုတော်တော်များများအတွက် 2FA ၁၂ ရက်တာ မှာ သွားကြည့်လို့ရပါတယ်။ Amazon၊ Bank of America၊ Dropbox၊ Facebook၊ Gmail နဲ့ Google၊ LinkedIn၊ Outlook.com နဲ့ Microsoft၊ PayPal၊ Slack၊ Twitter နဲ့ Yahoo Mail တို့မှာ 2FA ကို ဘယ်လို ဖွင့်ရမယ်ဆိုတာကို သေသေချာချာ ပြောပြပေးထားပါတယ်။

စကားဝှက်တွေ အခိုးခံရတာကနေ ကာကွယ်ချင်တယ်ဆိုရင် အဲဒီ့စာရင်းတွေကို သေသေချာချာဖြတ်ပြီး သင် ကာကွယ်ချင်တဲ့ အရေးကြီးတဲ့ အကောင့်တွေမှာ 2FA ကို ဖွင့်ပြီး သုံးလိုက်ပါ။