EFF'S SURVEILLANCE SELF-DEFENSE

အဆင့်နှစ်ဆင့်ဖြင့်
စစ်မှန်ကြောင်းသက်သေပြခြင်းကိုဘယ်လိုလုပ်ဆောင်မလဲ

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

LOCALIZATION LAB

အဆင့်နှစ်ဆင့်ဖြင့်
စစ်မှန်ကြောင်းသက်သေပြခြင်းကိုဘယ်လိုလုပ်ဆောင်မလဲ

နောက်ဆုံးစိစစ်သည့်ရက်စွဲ - ၂၀၂၁ ခုနှစ် ဧပြီ ၂၉ ရက်

မိမိသည် အကောင့်သုံးစွဲသူ အစစ်ဖြစ်ကြောင်း သက်သေခံသည့်စနစ်ဖြစ်တဲ့ "အဆင့်နှစ်ဆင့်ဖြင့် စစ်မှန်ကြောင်းသက်သေပြခြင်း (2FA)" ကို ဝန်ဆောင်မှုပေးသူထံမှ နည်းလမ်းမတူညီတဲ့ (၂) မျိုးဖြင့် ရယူအသုံးပြုနိုင်ပါတယ်။ အဲဒီနည်းလမ်းတွေထဲမှာ အသုံးပြုသူသာသိသော (စကားဝှက် (သို့) လျှို့ဝှက်နံပါတ်စဉ်)။ အသုံးပြုသူသာပိုင်ဆိုင်သည့် (ကုန်မာတိုကင် (သို့) မိုဘိုင်းဖုန်း) သို့မဟုတ် အသုံးပြုသူနဲ့ ဒွန်တွဲပြီးရှိနေတဲ့အရာ (ဥပမာ-လက်ဗွေ) စတာတွေကို အသုံးပြုတဲ့နည်းလမ်းတွေ ပါဝင်ပါတယ်။

သင့်ဘဝတလျှောက်မှာ 2FA ကို အသုံးပြု ဖူးပါလိမ့်မယ်။ ဥပမာအားဖြင့် အေတီအမ်မှငွေထုတ်တဲ့အခါ ဘဏ်ကဒ်နှင့် လျှို့ဝှက်နံပါတ်စဉ်နှစ်မျိုးကိုအသုံးပြုသလိုမျိုးပေါ့။ အွန်လိုင်းဝန်ဆောင်မှုအများစုမှာတော့ စကားဝှက်ကို အသုံးပြုတဲ့ အဆင့်တစ်ဆင့်ကိုပဲ အလိုအလျောက် အသုံးပြုလေ့ရှိတတ်ပါတယ်။

အွန်လိုင်းတွင် "အဆင့်နှစ်ဆင့်ဖြင့် စစ်မှန်ကြောင်းသက်သေပြခြင်း" (2FA) က ဘယ်လို အလုပ်လုပ်သလဲ။

ဖေ့စ်ဘုတ်၊ ဂူဂဲလ်နှင့် တွစ်တာတို့ကဲ့သို့သော အွန်လိုင်းဝန်ဆောင်မှုတွေမှာ 2FA ကို စကားဝှက်တစ်ဆင့်တည်းကို သုံးတဲ့ သက်သေခံနည်းလမ်းအစားသုံးနိုင်ပါတယ်။ 2FA ကို ဖွင့်ထားမယ်ဆိုရင် စကားဝှက်နဲ့အတူ အခြားနည်လမ်းတစ်ခုကိုပါသုံးပြီး သက်သေခံနိုင်ပါတယ်။ စကားဝှက်နဲ့ တွဲသုံးလေ့ရှိတဲ့ အခြားနည်းလမ်းကတော့ စာတိုကတဆင့်ပို့တဲ့တစ်ကြိမ်သာ အသုံးပြုနိုင်သောကုဒ် (သို့မဟုတ်) မိုဘိုင်းအက်ပ်စတိုးတွေကထုတ်ပေးတဲ့ တစ်ခါသုံး ကုဒ်ကိုဖြည့်သွင်းရသည့်နည်းလမ်း ဖြစ်လေ့ရှိပါတယ်။ ဘယ်နည်းလမ်းပဲဖြစ်ဖြစ် ပေးပို့လာတဲ့ တစ်ခါသုံးကုဒ်ကိုလက်ခံဖို့ သင့်မိုဘိုင်းဖုန်း (သို့မဟုတ်) သင်အမြဲတမ်း အသုံးပြုလေ့ရှိသည့် စက်ပစ္စည်းတစ်ခုခုကိုတော့သုံးရပါမယ်။ ဂူဂဲလ်အပါအဝင် အချို့ဝက်ဘ်ဆိုဒ်များကလည်း တစ်ခါသုံးအရံသင့်သုံးကုဒ်များကို ထုတ်လုပ်ပေးနိုင်ပါတယ်။ ၎င်းတို့ကို ဒေါင်းလုတ်ဆွဲပြီး စာရွက်ပေါ်တွင် ရိုက်နှိပ်ကာ စိတ်ချရတဲ့တနေရာမှာသိမ်းဆည်းပြီး အရံသင့်ဆောင်ထားနိုင်ပါတယ်။ 2FA ကို အသုံးပြုဖို့ရွေးချယ်လိုက်တာနဲ့ သင့်စကားဝှက်နှင့်တကွ အသင့်သုံးကုဒ်နံပါတ်ကို ဖုန်းမှာရိုက်ပြီး သင့်အကောင့်ထဲဝင်နိုင်ပါတယ်။

2FA ကို ဘာ့ကြောင့်သုံးသင့်လဲ။

2FA တွင် အကောင့်ပိုင်ရှင်အစစ်အမှန်ဟုတ်/မဟုတ်ကို နည်းလမ်းနှစ်မျိုးနဲ့ စစ်ဆေးပြီးမှ အကောင့်ထဲဝင်ခွင့်ပြုတာမို့ မိမိအကောင့်ကို ပိုမိုလုံခြုံမှုရှိစေပါတယ်။ အခြားသူလက်ထဲကို သင့်ရဲ့ စကားဝှက်ရောက်သွားရင်တောင်မှ သင့်ဖုန်း (သို့) အခြားသက်သေထူတဲ့နည်းလမ်းကို မသိဘူးဆိုရင် သင့်အကောင့်ထဲကို ဝင်လို့ရမှာမဟုတ်ပါဘူး။

2FA စနစ်၏ အားနည်းချက်များ။

2FA က အကောင့်ပိုင်ရှင်စစ်မှန်ကြောင်းသက်သေပြနိုင်သည့် ပိုမိုလုံခြုံစိတ်ချရသည့်နည်းလမ်းဖြစ်ပေမဲ့ သင်ကိုယ်တိုင် သင့်အကောင့်ထဲဝင်လို့မရတဲ့ အဖြစ်တွေလည်း ပိုကြုံလာရနိုင်ပါတယ်။ ဥပမာ သင့်ဖုန်းကျပျောက်ခြင်း၊ အထားမှားခြင်း၊ ဖုန်းနံပါတ်ပြောင်းခြင်း၊ roaming ဝန်ဆောင်မှုမဖွင့်ဘဲ နိုင်ငံတကာသို့ခရီးထွက်ခြင်း။

2FA ဝန်ဆောင်မှုမှ တစ်ခါသုံး “အရန်သင့်” သို့မဟုတ် “ပြန်လည်ကယ်ဆယ်သည့်” ကုဒ်အချို့ကို ထုတ်ပေးနိုင်ပါတယ်။ ကုဒ်တစ်ခုစီကို သင့်အကောင့်အတွင်းသို့ တစ်ကြိမ်ဝင်ရောက်ရန်သုံးနိုင်ပြီး နောက်အကြိမ်များအတွက်မူ ယင်းကုဒ်သည်အသုံးမဝင်တော့ပါ။ တကယ်လို့ သင့်အနေနဲ့ ဖုန်းပျောက်တာ (သို့) ဖုန်းကိုဆုံးရှုံးရနိုင်ခြေရှိတယ်ဆိုရင် ထိုတစ်ခါသုံးကုဒ်များကို စာရွက်နှင့်ထုတ်ပြီး မိမိနှင့်တပါတည်းယူဆောင် သွားပါ။ ကော်ပီတစ်စောင်သာထုတ်ပြီး ဘယ်သူမှမသိနိုင်တဲ့ လုံခြုံစိတ်ချရသောနေရာတွင်သိမ်းဆည်းပါ။ ထိုတစ်ခါ သုံးကုဒ်စာရင်း စာရွက်ပျောက်သွားခဲ့တယ်ဆိုရင် အကောင့်သို့ဝင်ရောက်သည့်အခါ နောက်ထပ်စာရင်းတစ်ခု ထပ်ထုတ်ပြီး သိမ်းဆည်းပါ။

2FA စနစ်ရဲ့အခြားအားနည်းချက်တစ်ခုမှာ SMS စာတိုပို့သည့်နည်းလမ်းက လုံခြုံစိတ်ချရမှု မရှိတဲ့အတွက် SMS စာတိုက အကောင့်ထဲ ဝင်ရောက်ဖို့ကြိုးစားသူရဲ့ စစ်မှန်မှုကို သက်သေခံတဲ့နည်းလမ်းအဖြစ် သုံးတာက ထင်သလောက် လုံခြုံစိတ်ချရမှုမရှိလို့ ဆိုနိုင်ပါတယ်။ မိုဘိုင်းဖုန်း ကွန်ယက်ထဲကို ဝင်ရောက်နိုင်သူလိုမျိုး အဆင့်မြင့်တိုက်ခိုက်သူများ (ဥပမာ ထောက်လှမ်းရေး အေဂျင်စီ သို့မဟုတ် ရာဇဝတ်ဂိုဏ်းများ) က သင့်အကောင့်ကို ဖွင့်ဖို့ကြိုးစားတာဆိုရင် SMS စာတိုမှ ပေးပို့သည် ကုဒ်များကို အလွယ်တကူရယူသွားနိုင်ပါတယ်။ အဆင့်မြင့်တိုက်ခိုက်သူ မဟုတ်ရင်တောင် အချို့သောဖုန်း ဝန်ဆောင်မှုများ ဖြစ်တဲ့ လိုင်းလွှဲခြင်းဝန်ဆောင်မှုကိုသုံးပြီး ဖုန်းခေါ်ဆိုမှု/ စာတိုပေးပို့မှုတွေကို တိုက်ခိုက်သူရဲ့ ဖုန်းနံပါတ်ထဲကို လမ်းလွှဲရောက်ရှိစေပြီး တပါးသူအကောင့်ကို ဖွင့်ခဲ့တဲ့ သာဓကတွေလည်း ရှိပါတယ်။

ထိုကဲ့သို့သောတိုက်ခိုက်မှုမျိုးဖြစ်ပေါ်လာမှာကို စိုးရိမ်ပါက SMS စာတိုနည်းလမ်းနဲ့ သက်သေခံခြင်းကို ပိတ်ပြီး Google Authenticator သို့ Authy တို့လိုမျိုး စစ်ဆေးသက်သေခံပေးတဲ့ အက်ပ်တွေကိုသာ အသုံးပြုပါ။ ဒါပေမဲ့ အဲဒီဝန်ဆောင်မှုတွေကလည်း 2FA ဝန်ဆောင်မှုတိုင်းအတွက် အသုံးမပြုနိုင်ပါ။

နောက်တစ်ချက်က 2FA ကိုအသုံးပြုလိုက်တဲ့အခါ မိမိပေးလိုတဲ့ ကိုယ်ရေးအချက်အလက်ထက်ပိုပေးသည့် သဘောလည်းသက်ရောက်သွားနိုင်ပါတယ်။ ဆိုလိုသည်မှာ တွစ်တာမှာအမည်ဝှက်နဲ့ မှတ်ပုံတင်ပြီး မိမိကိုယ်ရေးအချက်အလက်များကို လျှို့ဝှက်ပြီးသုံးခြင်း၊ Tor သို့ VPNအသုံးပြုပြီး တွစ်တာကို ဝင်ရင်တောင် SMS စာတိုနည်းလမ်းကိုအသုံးပြုတဲ့ 2FA စနစ်ကို ဖွင့်ထားမယ်ဆိုရင် ကိုယ့်ရဲ့မိုဘိုင်းဖုန်းနံပါတ်ကို တွစ်တာကို ပေးရမှာဖြစ်တယ်။ တကယ်လို့သင့် အကောင့်ကိုစစ်ဆေးဖို့ တရားရုံးမှ အမိန့်ချမှတ်မယ်ဆိုရင် သင့်ဖုန်းနံပါတ်ကိုသုံးပြီး သင့်အကောင့်ကို ခြေရာခံလိုက်နိုင်ပါလိမ့်မယ်။ သင့်အကောင့်ဟာ သင့်ကိုယ်ပိုင်နာမည်နှင့်မဟုတ်ဘဲ သင့်ကိုယ်ရေး အချက်အလက်နှင့် သင့်အမည်ကိုဝှက်ထားလိုလျှင် SMS စာတိုနည်းလမ်းကိုသုံး တဲ့ 2FA စနစ်ကို အသုံးပြုဖို့ အလွယ်တကူ ဆုံးဖြတ်ချက်မချပါနဲ့။

နောက်ဆုံးအချက်ကတော့ 2FA ကိုဖွင့်ပြီးတာနဲ့ အကောင့်ပိုင်ရှင်တွေက လွယ်ကူတဲ့ စကားဝှက်ကို ပြောင်းလဲအသုံးပြုကြတာကိုတွေ့ရှိရပါတယ်။ ဘယ်လိုအခြေအနေပဲဖြစ်ဖြစ် ခိုင်မာအားကောင်းတဲ့ စကားဝှက်ကို အသုံးပြုပါ။ ထိုကဲ့သို့စကားဝှက်ကို ဖန်တီးရန် creating strong passwords guide တွင် လေ့လာပါ။

2FA စနစ်ကို ဘယ်လိုရယူအသုံးပြုမလဲ။

ပလက်ဖောင်းတစ်ခုနှင့်တစ်ခုအပေါ်မူတည်၍ 2FA စနစ်နှင့်စကားလုံး အသုံးအနှုံးကွဲပြားပါတယ်။ https://twofactorauth.org/ တွင် 2FA စနစ်ကိုပံ့ပိုးသည့် ဆိုက်များစာရင်းကို ဝင်ရောက်ကြည့်ရှုနိုင်ပါတယ်။ အများသုံးဝန်ဆောင်မှုတွေဖြစ်တဲ့ Amazon, Bank of America, Dropbox, Facebook, Gmail and Google, LinkedIn, Outlook.com and Microsoft, PayPal, Slack, Twitter, နှင့် Yahoo Mail တို့အတွက် 2FA စနစ် ရယူခြင်းအတွက် 12 Days of 2FA post တွင် ကိုးကားနိုင်ပါတယ်။

စကားဝှက်များခိုးယူခံရလျှင် မိမိအကောင့်အား မဆုံးရှုံးစေရေးအတွက် ကာကွယ်ရေးနည်းလမ်းများကို သိရှိလိုလျှင် ဒီစာရင်းကို ဖတ်ရှုပြီး မိမိ၏ အရေးကြီးအကောင့်အားလုံးအတွက် 2FA စနစ်ကိုဖွင့်လှစ်အသုံးပြုပါ။