

EFF'S SURVEILLANCE SELF-DEFENSE

iPhone အားကုန်ဖြင့်ပြောင်းလဲခြင်းလုပ်ဆောင်နည်း

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



LOCALIZATION LAB

iPhone အားကုန်ဖြင့်ပြောင်းလဲခြင်းလုပ်ဆောင်နည်း

နောက်ဆုံးစိစစ်သည့်ရက်စွဲ - ၂၀၂၁ ခုနှစ် ဧပြီလ ၂၉ ရက်

သင့် iPhone သည် 3S (သို့) 3S နောက်ပိုင်းထွက်ရှိသောဖုန်းဖြစ်လျှင် (သို့) iPod တတိယမျိုးဆက် (သို့) နောက်ပိုင်းထွက်ရှိသော iPod ဖြစ်လျှင် (သို့) မည်သည့် iPad အမျိုးအစားဖြစ်စေ ၎င်းတို့ကို ကုန်ဖြင့် ပြောင်းလဲခြင်းနည်းလမ်းသုံးပြီး [စက်အတွင်းရှိ အချက်အလက်များရဲ့လုံခြုံရေးကို မြှင့်တင်နိုင်ပါတယ်။](#) ဆိုလိုသည်မှာ သင့်စက်ပစ္စည်းဟာ တစ်စုံတစ်ဦးရဲ့လက်ထဲ ရောက်ရှိသွားမယ်ဆိုရင် စက်အတွင်း သို့လှောင်ထားတဲ့ အချက်အလက်များဖြစ်တဲ့ ဖုန်းစာအုပ်၊ စာတိုများ၊ ဖုန်းခေါ်ဆိုမှုများနှင့် အီးမေးလ်စတာတွေကို စက်ဖွင့်တဲ့အခါသုံးတဲ့ စကားဝှက်မရှိဘဲ ဝင်ရောက်ကြည့်ရှုနိုင်မှာ မဟုတ်ပါဘူး။

နောက်ဆုံးပေါ် Apple စက်ပစ္စည်းများတွင် သို့လှောင်ထားတဲ့ ဖိုင်များရဲ့ လုံခြုံရေးအတွက် အလိုအလျောက် ကုန်ဖြင့်ပြောင်းလဲသည့်စနစ်ကိုထည့်သွင်းထားပါတယ်။ ဒါပေမယ့် သင်စက်ပစ္စည်းကို အရယူပြီး အချက်အလက်များခိုးခံရခြင်းမှ ကာကွယ်နိုင်ဖို့ကတော့ သင်တစ်ဦးတည်းသာ သိသည့် ဝှက်စာကြောင်း (သို့မဟုတ်) ကုန်ကို အသုံးပြုနိုင်ပါတယ်။ လုပ်ဆောင်နိုင်မယ့်နည်းလမ်းတွေအတွက် အောက်ပါလမ်းညွှန်ချက်များကို ကိုးကားပါ။

iOS 4 မှ iOS 7 အတွင်း အသုံးပြုသည့်စက်ပစ္စည်းများအတွက် လမ်းညွှန်

- ၁။ General settings ကိုဖွင့်ပါ။ Passcode (သို့မဟုတ်) iTouch & Passcode ကိုရွေးပါ။
- ၂။ ညွှန်ကြားချက်များအတိုင်း လျှို့ဝှက်ကုန်ကို ရိုက်သွင်းပါ။

iOS 8 မှ iOS 11 အတွင်းအသုံးပြုသည့် စက်ပစ္စည်းများအတွက် လမ်းညွှန်

- ၁။ Settings app ကိုဖွင့်ပါ။
- ၂။ Touch ID & Passcode ကို ဖိပါ။
- ၃။ ညွှန်ကြားချက်များအတိုင်း လျှို့ဝှက်ကုန်ကို ရိုက်သွင်းပါ။

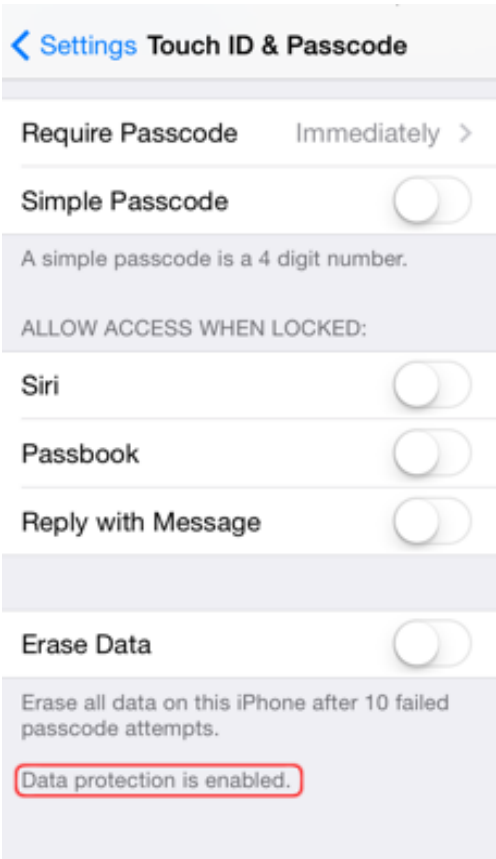
သင့်စက်သည် iOS 8 စနစ်ကို သုံးလျှင် Simple Passcode ကိုပိတ်၍ ဂဏန်း ၄ လုံးထက်ပိုသော လျှို့ဝှက်ကုန် ကိုထည့်သွင်းပါ။ iOS 9 စနစ်မှစပြီး Apple ပစ္စည်းများတွင် ဂဏန်း ၆ လုံးသုံး လျှို့ဝှက်ကုန်ကိုသာ အသုံးပြုပါ။

သင့်အနေနဲ့ ကိန်းဂဏန်းနဲ့ရေးတဲ့လျှို့ဝှက်ကုန်ကိုသုံးမယ်ဆိုရင် ဖုန်းဖွင့်ချိန်မှာ ကိန်းဂဏန်းများသာပါ ရှိတဲ့ လက်ကွက်ပေါ်လာပါလိမ့်မယ်။ ကိန်းဂဏန်းက စာလုံးများ၊ သင်္ကေတများနှင့် ကိန်းဂဏန်း များ

ရောထားတဲ့ စကားဝှက်ကို လက်ကွက်သေးသေးလေးပေါ်မှာ ရိုက်ထည့်ရတာထက် ပိုပြီးလွယ်ကူပါတယ်။ ဒါပေမဲ့ လုံခြုံရေးရှုထောင့်က ကြည့်ရင်တော့ စာလုံးနှင့် ကိန်းဂဏန်းတွေနဲ့ရောရေးထားတဲ့ စာလုံးရေ ၆ လုံး ထက်ပိုတဲ့ စကားဝှက်ကို အသုံးပြုဖို့ အကြံပြုပါတယ်။ ဒါ့အပြင် Apple ရဲ့ စက်ပစ္စည်းတွေဟာ စကားဝှက်ဖော်သည့် နည်းပညာအသုံးပြုဖွင့်ခြင်းကို နှောင့်နှေးစေပေမဲ့ ခက်ခဲတဲ့ စကားဝှက်ကိုသုံးထားရင်တော့ ဖုန်းသော့ကိုဖွင့်ဖို့ ပိုပြီးခက်ခဲစေပါလိမ့်မယ်။

သင့် စိတ်တိုင်းကျ စကားဝှက်ကို ထည့်သွင်းနိုင်ဖို့ “Passcode Options” နှင့် “Custom Alphanumeric Code” ကိုရွေးပါ။ အကယ်၍ သင့်လက်ရှိစကားဝှက်ကို ပြောင်းလိုပါက “Change Passcode” ကိုရွေးပြီးနောက် “Passcode Options” ကိုဆက်ရွေးပါ။ “Require passcode” တွင် “Immediately” ကိုပြောင်းပါ။ သင့်ဖုန်းမသုံးသည့်အချိန်တွင် အလိုအလျောက်ဖုန်းလော့ခံကျသွားစေရန် ဖြစ်ပါတယ်။

စကားဝှက်ထည့်သွင်းပြီးရင်တော့ Passcode setting စာမျက်နှာအောက်ဆုံးသို့သွားပါ။ “Data protection is enabled” ဆိုသည့်စာကြောင်းကိုတွေ့ပါလိမ့်မယ်။ ဆိုလိုသည်မှာသင့်ဖုန်းကိုကုန်ဖြင့်ပြောင်းလဲသည့်စနစ်ဖြင့် ချိတ်ဆက်ထားလိုက်ပြီ ဖြစ်တဲ့အတွက် သင့်စကားဝှက်ကို မသိဘဲ သင့်ဖုန်းပါအချက်အလက်များကိုကြည့်ရှုနိုင်တော့မည်မဟုတ်ပါ။



သင့်ကိုယ်ရေးအချက်အလက်လုံခြုံမှုအတွက် အောက်ပါ iOS လုပ်ဆောင်ချက်များကို သတိထားပြီးအသုံးပြုပါ -

- iTunes တွင် သင့်အချက်အလက်များကို [ကွန်ပျူတာအတွင်းသို့ပုံတူပွားနိုင်တဲ့ ဝန်ဆောင်မှု](#) ရှိပါတယ်။ ပုံတူပွားအချက်အလက်များကို ကုဒ်ဖြင့်ပြောင်းလဲခြင်းကို iTunes မှ အလိုအလျောက် မလုပ်ဆောင်ပေးပါ။ ဒါ့ကြောင့် iTunesရဲ့ Summary ခလုတ်မှ “Encrypt backup” ကိုရွေးချယ်မှသာ ဝိုင်ဖိုင်စကားဝှက်နှင့် အီးမေးလ်စကားဝှက်ကဲ့သို့သော အရေးကြီးသည့် အချက်အလက်တွေကို ကုဒ်ဖြင့်ပြောင်းလဲပြီးမှ ကွန်ပျူတာအတွင်း သိမ်းဆည်းပေးမှာ ဖြစ်ပါတယ်။ အသုံးပြုသည့် စကားဝှက်ကို လုံခြုံသည့်နေရာတွင် သိမ်းဆည်းမှတ်သားထားပါ။ ပုံတူပွားအချက်အလက်များကို ပြန်လည်ရယူတာမျိုးက ဖြစ်လေ့ဖြစ်ထမရှိပေမဲ့ စကားဝှက် ပျောက်ဆုံးသွားရင်တော့ အရေးပေါ်အခြေအနေမှာ အချက်အလက်များရယူနိုင်မည်မဟုတ်ပါ။
- ပုံတူပွားအချက်အလက်တွေကို iCloud အတွင်း သိမ်းဆည်းလိုပါက ရှည်လျားသော စကားဝှက်ဖြင့် သိမ်းဆည်းပါ။ Apple က ပုံတူပွားအချက်အလက်အတော်များများကို ကုဒ်ဖြင့်ပြောင်းလဲပေးနိုင်ပေမဲ့ အဲဒီကုဒ်တွေကိုပြန်ဖြည့်တဲ့ သော့ကိုထိန်းချုပ်တဲ့ ခလုတ်တွေကိုပါ ပိုင်ဆိုင်တဲ့အတွက် လုံခြုံရေးအဖွဲ့တွေက Appleကို ဖိအားပေးပြီး သင့်စက်ပစ္စည်းကိုဖွင့်ခိုင်းမယ်ဆိုရင် ရှည်လျားခက်ခဲသောစကားဝှက်က သော့ဖွင့်ပေးဖို့ အခက်အခဲကြုံတွေ့စေမှာပါ။
- သင့်စက်ပစ္စည်းအတွင်းရှိအချက်အလက်များကို အထက်မှာ ဖော်ပြခဲ့တဲ့ အဆင့်ဆင့်အတိုင်း ဆောင်ရွက်ထားမယ်ဆိုရင် အရေးပေါ်အခြေအနေမှာ အချက်အလက်တွေကို လုံခြုံစိတ်ချစွာ ပယ်ဖျက်နိုင် ပါလိမ့်မယ်။ Touch ID & Passcode settings တွင် စကားဝှက်ကို ၁၀ ကြိမ်မှားနိုင်လျှင် အချက်အလက်များအားလုံး အလိုအလျောက်ပယ်ဖျက်သည့် လုပ်ဆောင်ချက်ကို ဖွင့်ထားနိုင်ပါတယ်။ အဲဒီလိုမလုပ်ခင် သင့်အချက်အလက်တွေကို အခြားတစ်နေရာမှာ ပုံတူပွားသိမ်းဆည်းထားဖို့မမေ့ပါနှင့်။ သို့မှသာ အခြားသူတစ်ဦးက သင့်ဖုန်းအတွင်းရှိအချက်အလက်များပျက်စီးစေလိုတဲ့ ရည်ရွယ်ချက်နဲ့ သင့်ဖုန်းမှာ စကားဝှက်အမှားတွေကို ထပ်ခါထပ်ခါ နှိပ်မှာကို စိုးရိမ်စရာမလိုတော့ပါ။
- [Apple's old Law Enforcement Guide](#) Apple ရဲ့ ဥပဒေလမ်းညွှန်အဟောင်းမှာဆိုရင် Apple က စကားဝှက်ဖြင့်သော့ခတ်ထားသည့် iOS စက်ပစ္စည်းများမှ အချို့အချက်အလက်များကို ဆွဲထုတ်နိုင်ပါတယ်။ အထူးသဖြင့် Apple စက်ပစ္စည်းများအတွင်း မူရင်းပါဝင်သည့် အက်ပလီကေးရှင်းများထဲကို သုံးစွဲသူမှထည့်သွင်းထားသော ဖိုင်များနဲ့ ကုဒ်ဖြင့်ပြောင်းလဲ ထားသည့်စနစ်ကိုအသုံးမပြုထားသည့် အချက်အလက်များကို လုံခြုံရေး အဖွဲ့အစည်းများက ဥပဒေအရတောင်းဆိုမှုလုပ်ရင် ဖော်ထုတ် မျှဝေနိုင်ပါတယ်။ iOS 4 နှင့် ၎င်းထက်မြင့်သော ဗားရှင်းများမှာ အဲဒီလိုလုပ်လို့ရပါတယ်။ အထူးသတိပြုရမည်မှာ ဂရုစိုက်မှုနှင့်ဝရမ်းဖြင့် အချက် အလက်များကို ဆွဲထုတ်ရင်တောင်မှ သုံးစွဲသူမှထည့်သွင်းထားသော ဖိုင်များဖြစ်သည့်

စာတိုများ၊ ဓါတ်ပုံများ၊ ဗီဒီယိုများ၊ ဖုန်းစာအုပ်၊ အသံသွင်းမှုများနှင့် ဖုန်းခေါ်ဆိုမှုစာရင်းတို့ကိုသာ Apple မှ ဆွဲထုတ်ပေးနိုင်မှာဖြစ်ပြီး သင့်အီးမေးလ်၊ ပြက္ခဒိန်တွင်မှတ်သားထားသည့်အချက်အလက်များနှင့် အခြား အက်ပလီကေးရှင်းများမှ အချက်အလက်များကိုမူ ဆွဲထုတ်ပေးနိုင်မှာမဟုတ်ပါဘူး။

ယခုဖော်ပြခဲ့တဲ့ အချက်အလက်တွေဟာဆိုရင် iOS 8.0 မတိုင်ခင်က ဗားရှင်းတွေကိုသုံးတဲ့ iOS စက်ပစ္စည်းတွေအတွက် ဖြစ်ပါတယ်။

- “iOS8 နောက်ပိုင်းထွက်ရှိသော စက်ပစ္စည်းတွေ အတွက်ကတော့ကုန်ဖြင့်ပြောင်းလဲထားခြင်းကို ဖြည့်ထုတ်နိုင် သည့်သော့ခလုတ်ကို Apple မှပိုင်ဆိုင်ခြင်းမရှိတာမို့ လုံခြုံရေး အဖွဲ့အစည်းများ ကတောင်းသည့်တိုင် ဘယ်လိုအချက်အလက်ကိုမျှဆွဲ ထုတ်ပေးနိုင်ခြင်းမရှိ” ဟု [Apple ကဆိုပါတယ်။](#)

အထူးသတိပြုရမည့်အချက်၊ ဖုန်းတွင်းကအချက်အလက်များကို Apple မှ ဆွဲထုတ်ပေးနိုင်စွမ်းမရှိသည့် တိုင် သင့်ဖုန်းပါအချက်အလက်များကို သင့်ကွန်ပျူတာ (သို့မဟုတ်) iCloud တွင် ပုံတူပွားသိမ်းဆည်းထားပါက ထိုနေရာများမှတစ်ဆင့် အချက်အလက်များကို ဝင်ရောက်ရယူနိုင်သည်ကို သတိပြုပါ။ ကုန်ဖြင့် ပြောင်းလဲခြင်းနည်းစနစ်ဟာ ဖုန်းပိတ်ထားသည့်အချိန် (သို့မဟုတ်) ဖုန်းကို ပြန်စသည့်အချိန် (သော့ခလုတ်မဖွင့်ရသေးချိန်) တွင် အထိရောက်ဆုံးဖြစ်ပါတယ်။ အချို့သော အချက်အလက်ခိုးယူ သူများဟာ ဖုန်းဖွင့်ထားချိန်မှာ သင့်စက်ပစ္စည်းမှတ်ဉာဏ်မှ အချက်အလက်များကိုရယူဖို့ လုပ်ဆောင်ကြပါတယ်။ တကယ်လို့ သင့်ဖုန်းအခိုးခံရလျှင် (သို့မဟုတ်) အသိမ်းခံရလျှင် သင့်ဖုန်းပါဝါပိတ် နိုင်အောင် (သို့မဟုတ်) ပြန်စသည့်အနေအထားရောက်အောင် လုပ်ဆောင်ပါ။ ယခု လမ်းညွှန်ရေးသားနေစဉ်အတွင်း အချို့ကုမ္ပဏီများက လုံခြုံရေး အဖွဲ့အစည်းများရဲ့ တောင်းဆိုမှုအတိုင်း အချို့သော iPhone များ၏ စကားဝှက်များကို အောင်မြင်စွာဖော်ထုတ်ပေးနိုင်ပြီဖြစ်ကြောင်း ကြေငြာထားပေမဲ့ အသေးစိတ်ကိုမူ မသိရှိရသေးပါ။

- သင့် Apple စက်ပစ္စည်း အခိုးခံရခြင်း(သို့မဟုတ်) ပျောက်ဆုံးသွားလျှင် ၎င်း စက်ပစ္စည်းအတွင်းရှိ အချက်အလက်များကို “Find My iPhone” လုပ်ဆောင်ချက်နဲ့ အဝေးမှ ပယ်ဖျက်နိုင်ပါတယ်။ အဲဒီ လုပ်ဆောင်ချက်ကြောင့် Apple မှ သင့်ဖုန်းတည်နေရာကို အချိန်မရွေးခြေရာခံနိုင်တဲ့ အနေအထားလည်းရှိပါတယ်။ အဲဒီလုပ်ဆောင်ချက်ကို ဖွင့်၊ မဖွင့်စဉ်းစားတဲ့အခါမှာ သင့်ဖုန်းပျောက်ဆုံးသွားရင် ဖုန်းတွင်းအချက်အလက်များကို အဝေးမှဖျက်နိုင်သဖြင့်ရရှိမည့်အ ကျိုးကျေးဇူးနှင့် မိမိတည်နေရာကို အချိန်မရွေးရှာဖွေသိရှိနိုင်သည်ဆိုသည့် ဆိုးကျိုးတို့အကြား ချိန်ထိုးစဉ်းစားရမှာ ဖြစ်ပါတယ်။ (တယ်လီကွန်းနှင့်ချိတ်ဆက်သည့် မိုဘိုင်းဖုန်းများကသာ တည်နေရာကို အချိန်ပြည့်ထုတ်လွှတ်နိုင်ပြီး ဝိုင်ဖိုင်အသုံးပြုသည့် iPad နှင့် iPod Touchများကမူ တည်နေရာကို အချိန်ပြည့်မထုတ်လွှတ်နိုင်ပါ။)