EFF'S SURVEILLANCE SELF-DEFENSE

ဖစ်ရှင်းနည်းလမ်းနဲ့ တိုက်ခိုက်မှုတွေကို ဘယ်လိုရှောင်ရှားမလဲ

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

LOCALIZATION LAB

ဖစ်ရှင်းနည်းလမ်းနဲ့ တိုက်ခိုက်မှုတွေကို ဘယ်လိုရှောင်ရှားမလဲ

နောက်ဆုံးစိစစ်သည့်ရက်စွဲ - ၂၀၂၁ ခုနှစ်၊ မေလ ၂၈ ရက်

ဒီဂျစ်တယ်လုံခြုံရေးမြှင့်တင်ရာမှာ မကောင်းတဲ့သူအချို့က သင့်ရဲ့ လုံခြုံမှုကျိုးပေါက်အောင် ကြိုးပမ်းတာကို အနည်းနဲ့ အများတော့ မလွဲမသွေကြုံရတတ်ပါတယ်။ ဒီလိုလုပ်တဲ့သူတွေကို ရန်ဘက်(adversaries) လို့ခေါ်ပါတယ်။ ရန်ဘက် adversary တစ်ယောက်က ကိုယ့်ဆီ သာမန်လို့ ထင်ရတဲ့ အီးမေးလ် (သို့မဟုတ်) လင့်ခ်တစ်ခုခုကို ပို့မယ်။ တကယ်က အဲဒီ အီးမေးလ် (သို့မဟုတ်) လင့်ခ်က ကိုယ့်ဒီဂျစ်တယ်လုံခြုံရေးကို တိုက်ခိုက်အောင်ဖန်တီးထားတာမျိုးဖြစ်တယ်။ အဲဒီနည်းလမ်း နဲ့ တိုက်ခိုက်တာကို ဖစ်ရှင်းလို့ခေါ်ပါတယ်။

များသောအားဖြင့် ဖစ်ရှင်းတိုက်ခိုက်မှု attack မှာ သင့်ကို အောက်ပါအချက်တွေထဲက တစ်ခုကို လုပ်ခိုင်းတဲ့ မက်ဆေ့ချ်ပါလာတတ်ပါတယ်။

- ပါလာတဲ့လင့်ခ်ကိုနှိပ်ဖို့
- ပါလာတဲ့စာရွက်စာတမ်းကို ဖွင့်ဖို့
- ဆော့ဖ်ဝဲလ်ကို သင့်စက်ပစ္စည်းထဲတပ်ဆင်ဖို့နဲ့
- သင့် အသုံးပြုသူအမည်နဲ့ စကားဝှက်password ကို တရားဝင်လို့ထင်ရတဲ့ ဝက်ဘ်ဆိုက်တစ်ခုခုထဲ ရိုက်ထည့်ဖို့ စတာတွေပါတတ်ပါတယ်။

ဖစ်ရှင်းတိုက်ခိုက်မှုတွေက သင့်စကားဝှက်ပေးဖို့ (သို့မဟုတ်) malware ကို သင့်စက်ပစ္စည်း ထဲသွင်းဖို့ လှည့်ဖျားလုပ်ဆောင်စေပါတယ်။ သူတို့ခိုင်းတဲ့အတိုင်းသင်လုပ်မိလိုက်တာနဲ့ တိုက်ခိုက်သူတွေက malware ကိုသုံးပြီး သင့်စက်ပစ္စည်းကို အဝေးကနေထိန်းချုပ်တာပြီး သတင်းအချက်အလက် တွေခိုးတာမျိုး ဒါမှမဟုတ်၊ သင့်ကို စောင့်ကြည့်ထောက်လှမ်းတာမျိုးတွေလုပ်မှာပါ။

ဒီလမ်းညွှန်မှာတော့ ဖစ်ရှင်းတိုက်ခိုက်မှုတွေကိုဘယ်လိုရှာဖွေဖော်ထုတ်မလဲဆိုတာနဲ့ ကာကွယ်နိုင်တဲ့ နည်းလမ်းအချို့ကို တင်ပြပေးသွားပါမယ်။

ဖစ်ရှင်းတိုက်ခိုက်မှုအမျိုးအစားများ

စကားဝှက်များပေးရန် လှည့်ဖျားသည့် ဖစ်ရှင်းတိုက်ခိုက်မှု (ကိုယ်ရေးအချက်အလက်များရယူခြင်း)

သင့်ဆီကို လှည့်ဖျားဖန်တီးထားတဲ့လင့်ခ်တွေပို့ပြီး သင့်ဆီက စကားဝှက်ကိုရယူဖို့ကြိုးစားတဲ့နည်းလမ်းဖြစ်ပါတယ်။ မက်ဆေ့ချ်မှာပါတဲ့ ဝက်ဘ်လိပ်စာကတစ်မျိုးဖြစ်ပြီး တကယ်တမ်းကျ အခြားနေရာတစ်ခုဆီခေါ်သွားတာမျိုးပါ။ လင့်ခ်မှာပါတဲ့ ဝက်ဘ်တည်နေရာ URL ကို သင့်ကွန်ပျူတာပေါ်မှာများသောအားဖြင့် တွေ့ရပါတယ်။ ဒါပေမဲ့ အဲဒီလင့်ခ်မှာပါတဲ့ စကားလုံးတွေက တကယ့်ဝက်ဘ်ဆိုက်မှာပါတဲ့ စာလုံးတူတွေနဲ့ဖန်တီးထားတာမျိုး၊ စာလုံး တစ်လုံးလောက်ပြောင်းပြီး ဆင်တူယိုးမှားနာမည်ဖြစ်အောင် ရေးထားတာမျိုးတွေဖြစ်နေတတ်ပြီး သင်သုံးနေကျဝန်ဆောင်မှုတွေဖြစ်တဲ့ Gmail/Dropbox တို့လိုမျိုးဆီသွားတဲ့ လင့်ခ်လိုမျိုးဖြစ်အောင် ဖန်တီးထားတာပါ။ ဒီအတုအယောင် login စာမျက်နှာတွေက တကယ့်တရားဝင်အစစ်အမှန်တွေနဲ့ ဆင်တူလွန်းတာကြောင့် သင့်အနေနဲ့ အသုံးပြုသူအမည်နဲ့ စကားဝှက် password ကို သတိမပြုမိဘဲ ရိုက်ထည့်လိုက်မိနိုင်ပါတယ်။ သင်ရိုက်ထည့်လိုက်တာ နဲ့သင့်အချက်အလက်တွေကို တိုက်ခိုက်သူတွေက ရသွားမှာပါ။

ဒါ့ကြောင့် သင်ဘယ်စကားဝှက်ကိုမဆိုမရိုက်ထည့်ခင်မှာ သင့်ဝက်ဘ်ဘရောက်ဇာ web browser ကလိပ်စာဘားကို သေချာကြည့်ပါ။ အဲဒီမှာ ပေ့ချ်ရဲ့ ဒိုမိန်းနာမည် domain name အစစ်ကိုမြင်ရပါလိမ့်မယ်။ သင် login ဝင်နေတဲ့ ဆိုက်နဲ့ ပေါ်နေတဲ့ ဒိုမိန်းနာမည်နဲ့ မတူဘူးဆိုရင် ဆက်မလုပ်ပါနဲ့။ ကော်ပိုရိတ်စီးပွားရေးတံဆိပ်ပါရုံနဲ့ ပေ့ချ်ကအစစ်အမှန်လို့ မယူဆနိုင်ပါဘူး။ ဘယ်သူမဆို ပေ့ချ်အစစ်ဆီက တံဆိပ် (သို့မဟုတ်) ဒီဇိုင်းကိုခိုးကူးပြီး လိမ်ညာလှည့်ဖျားဖို့ လုပ်ဆောင်နိုင်ပါတယ်။

အချို့ကျတော့ နာမည်ကြီးဝက်ဘ်ဆိုက်လိပ်စာတွေနဲ့ ထင်ယောင်ထင်မှားဖြစ်အောင်လုပ်ထားတဲ့ လိပ်စာတွေနဲ့ သင့်ကို လှည့်ဖျားဖို့ ကြိုးစားပါလိမ့်မယ်။ https://wwwpaypal.com/ နဲ့ https://www.paypal.com/ ကွာသလိုပေါ့။ ဒီလိုပဲ paypal မှာ ပါတဲ့ “l”အစား “i” အကြီးကိုသုံးပြီးတော့ ရေးထားတဲ့ https://www.paypal.com/ နဲ့ https://www.paypal.com/ ကလည်း မတူပါဘူး။ လူအများစုက URL အရှည်တွေ ဖတ်ရလွယ်/ ရေးရလွယ်အောင် အတိုကောက်ရေးတာမျိုးရှိပေမဲ့ အချို့ကျတော့ တိုက်ခိုက်မှုတွေကို ဖွက်ထားဖို့သုံးတတ်ကြပါတယ်။ သင့်အနေနဲ့ တွစ်တာအတွက် အတိုကောက် URL ဖြစ်တဲ့ t.co လင့်ခ်လိုမျိုးရခဲ့ရင် https://www.checkshorturl.com/ နဲ့ တိုက်စစ်ပြီး ဘယ်ဝက်ဘ်ဆိုက်ထဲရောက်သွားလဲဆိုတာ အရင်စစ်ကြည့်သင့်ပါတယ်။

နောက်တစ်ခုသတိပြုရမှာက ပြန်စာပို့ရမယ့်လိပ်စာတွေကို အီးမေးလ်အတုနဲ့ ထင်ယောင်ထင်မှားဖြစ်အောင်လုပ်ဖို့ သိပ်လွယ်ပါတယ်။ ဒါ့ကြောင့် သင့်ဆီ အီးမေးလ်ပို့တဲ့သူက အဲဒီလိပ်စာနဲ့ သင့်ဆီကို တကယ်ပို့ထားသလားဆိုတာကို အီးမေးလ်ကြည့်ရုံနဲ့ အတည်ပြုလို့မရဘူးဆိုတာပါပဲ။

လူတစ်ယောက်တည်းကို ဦးတည်တိုက်ခိုက်သည့် လှံစွပ်ပစ်ဖစ်ရှင်းနည်းလမ်း

ဖစ်ရှင်းတိုက်ခိုက်မှုအများစုက ကွန်နဲ့ငါးဖမ်းသလို လူအစုလိုက်အပြုံလိုက်ကို လှည့်ဖျားဖို့ လုပ်ကြပါတယ်။ တိုက်ခိုက်သူအနေနဲ့ လူရာထောင်ချီထံကို အီးမေးလ်ပို့ပြီး စိတ်ဝင်စားစရာ ဗီဒီယိုတစ်ခုကိုဖွင့်ကြည့်ဖို့၊ အရေးကြီးစာရွက်စာတမ်းပို့ပေးတာ၊ ဒါမှမဟုတ် ဘေလ်ပေးတာနဲ့ ပတ်သက်လို့ ပြဿနာရှိနေတယ်ဆိုတာမျိုးတွေကို ပေးပို့တတ်ပါတယ်။

ဒါပေမယ့် တခါတလေကျတော့ တစ်ဦးတစ်ယောက်တည်းကိုရည်ရွယ်ပြီးတိုက်ခိုက်တတ်ပါတယ်။ အဲ့လို အခါမျိုးကျတော့ တိုက်ခိုက်သူက တိုက်ခိုက်ခံရမယ့်သူအကြောင်းကို သိပြီး အဲဒီ အချက် အလက်တွေကို သုံးပြီးတိုက်ခိုက်တာမျိုးပေါ့။ အဲ့ဒါကို “လူတစ်ဦးတစ်ယောက်တည်းကို ရည်ရွယ်ပြီး တိုက်ခိုက်တဲ့ လှံစွပ်ပစ်ဖစ်ရှစ်နည်းလမ်း (“spear phishing”) လို့ခေါ်ပါတယ်။ နမူနာပြောရရင် သင့်ဦးလေး ဘောရစ်ဆီကနေ သူ့ကလေးတွေရဲ့ ဓါတ်ပုံပို့ပေးလိုက်ကြောင်း အီးမေးလ်ရတယ်ဆိုပါတော့။ သင့်ဦးလေး နာမည်လည်းဟုတ်တယ်၊ သူ့မှာကလေးတွေလည်းရှိတယ်၊ အီးမေးလ်လိပ်စာကလည်း သူ့ဆီက လို့ထင်ရတယ်ဆိုရင် သင်ဖွင့်မိမှာပဲလေ။ အီးမေးလ်ဖွင့်လိုက်တော့ pdf ဖိုင်က တွဲလျက်ပါလာတယ်။ အဲဒီဖိုင်ကိုထပ်ဖွင့်တော့ သင့်ဦးလေးရဲ့ကလေးပုံတောင်ဖြစ်နေနိုင်သေးတယ်။ အဲဒီပုံနဲ့တွဲလျက်မှာ malware ကို ဝှက်ထည့်ပေးလိုက်တယ်။ သင်ပုံကိုဖွင့်ကြည့်လိုက်တာနဲ့ သင့်ရဲ့လုပ်ဆောင်ချက်တွေ အားလုံးကို အဲဒီ malware ကြောင့် စောင့်ကြည့်ထောက်လှမ်းလို့ရသွားမယ်။ သင့်ဦးလေးကသင့်ကို အီးမေးလ်ပို့တာမဟုတ်ဘဲ သင့်မှာဘောရစ်ဆိုတဲ့ဦးလေးနဲ့ အဲဒီဦးလေးမှာ ကလေးတွေရှိတာကို သိတဲ့သူ တစ်ဦးဦးကပို့တာဖြစ်တယ်။ သင့်အနေနဲ့ pdf ဖိုင်ကို ဖွင့်လိုက်တာနဲ့ pdf reader ကို သင့်ကွန်ပျူတာက ဖွင့်ဖို့ကြိုးစားတာကို အခွင့်ကောင်းယူပြီး ဆော့ဖ်ဝဲလ်မှာ ပါလာတဲ့ bug က သူဆီက ကုဒ်ကို သင့်ကွန်ပျူတာမှာ အလုပ်လုပ်စေတာဖြစ်တယ်။ ရလဒ်က pdf ဖိုင်ကိုဖွင့်ရင်းနဲ့ malware ကို ပါ ဒေါင်းလုတ်ဆွဲပြီးဖြစ်သွားပါတယ်။ အဲဒီ malware သင်နဲ့ ချိတ်ဆက်နေတဲ့သူတွေ၊ သင့်စက်ပစ္စည်း မှာပါတဲ့ ကင်မရာနဲ့ မိုက်ခရိုဖုန်းတွေကိုဖွင့်ပြီး မြင်သမျှ ကြားသမျှကို မှတ်တမ်းတင်ခိုးယူနိုင်ပါတယ်။

ဒါ့ကြောင့် အကောင်းဆုံးကာကွယ်နည်းကတော့ ပါလာတဲ့ လင့်ခ်တွေ၊ ဖိုင်တွေကို ဘယ်တော့မှ မဖွင့်မိစေဖို့ပါပဲ။ ဒါပေမဲ့ အဲ့ဒီအကြံကလည်း လက်တွေ့ကျမနေပြန်ဘူး။ ဒါ့ကြောင့် ဖစ်ရှင်းတိုက်ခိုက်မှုတွေကို လက်တွေ့ကျကျကာကွယ်နိုင်မယ့်နည်းလမ်းအချို့ကို အောက်မှာဆက်လက်ဖတ်ရှုနိုင်ပါတယ်။

ဖစ်ရှင်းတိုက်ခိုက်မှုကို ဘယ်လိုကာကွယ်မလဲ။

သင့်ဆော့ဖ်ဝဲလ်တွေကို နောက်ဆုံးဗားရှင်းဖြစ်အောင် အက်ပ်ဒိတ်လုပ်ပါ။

malware ကို သုံးတဲ့ ဖစ်ရှင်းတိုက်ခိုက်မှုအများစုက software bugs ကိုသုံးပြီးသင့်စက်ပစ္စည်းထဲ ရောက်အောင်လုပ်ပါတယ်။ အများအားဖြင့် bug ရှိကြောင်းသိတာနဲ့ ထုတ်လုပ်သူတွေက အဲဒါကို ဖယ်ဖို့ ဆော့ဖ်ဝဲလ်ကို အက်ပ်ဒိတ်လုပ်ပါတယ်။ ဒါ့ကြောင့် ဆော့ဖ်ဝဲလ်ဗားရှင်းအဟောင်းတွေမှာ malware တွေကို ပိုထည့်သွင်းလို့လွယ်ပါတယ်။ သင့်ဆော့ဖ်ဝဲလ်ကို အက်ပ်ဒိတ်လုပ်ထားရင် malware အန္တရာယ်ကို လျှော့ချနိုင်ပါတယ်။

အလိုအလျောက်ဖြည့်ပေးတဲ့ password manager ကို သုံးပါ။

Password managers စကားဝှက်မန်နေဂျာတွေက စကားဝှက်တွေကို အလိုအလျောက် ဖြည့်ပေးခြင်းဖြင့် ဘယ်ဆိုက်တွေက ဘယ်စကားဝှက်ကိုသုံးသလဲဆိုတာကို မှတ်တမ်းတင်ထားပါတယ်။ သာမန်လူတယောက်က ထင်ယောင်ထင်မှားလုပ်ထားတဲ့ ပေ့ချ်တွေကို တကယ့်အစစ်တွေနဲ့ မှားနိုင်ပေမဲ့ password စကားဝှက်မန်နေဂျာကိုတော့ လှည့်ဖျားဖို့ မစွမ်းနိုင်ပါဘူး။ တကယ်လို့ သင့်အနေနဲ့ စကားဝှက်မန်နေဂျာ (ဘရောက်ဇာနဲ့ပါတွဲသုံးတဲ့စကားဝှက်မန်နေဂျာ)ကို သုံးနေရင်း၊ ဆိုက်တစ်ခုခုကို စကားဝှက်အလိုအလျောက်မဖြည့်ပေးတော့ဘူးဆိုတာနဲ့ သင့်အနေနဲ့ အဲဒီဆိုက်ကို ဝင်မဲ့အစား သေချာအောင် အရင်စစ်ဆေးသင့်ပါတယ်။ နောက်တစ်ခုက ကျပန်းထုတ်ထားတဲ့ စကားဝှက်တွေဖြစ်တာမို့ အလိုအလျောက်ဖြည့်တာကို အားထားရမှာဖြစ်လို့ အတုအယောင် login ပေ့ချ်ထဲကိုယ့်ဘာကိုစကားဝှက်ရိုက်ထည့်ဖို့ဆိုတာလည်း ဖြစ်နိုင်ချေ နည်းသွားပါတယ်။

အီးမေးလ်ပို့သူတွေထံက ပို့ကြောင်းအတည်ပြုချက်ရယူပါ။

အီးမေးလ်ကတဆင့် ဖစ်ရှင်းတိုက်ခိုက်မှုလုပ်တာကို သိနိုင်ဖို့က အီးမေးလ်ပို့သူက တကယ်ပို့လားဆိုတာနဲ့ပတ်သက်ပြီး နည်းလမ်းပေါင်းစုံနဲ့ အတည်ပြုချက်ရယူဖို့လိုပါတယ်။ တကယ်လို့အီးမေးလ်ကို သင့်ဘဏ်က ပို့တယ်ဆိုရင် မဖွင့်သေးဘဲ သင့်ဘဏ်ကို အရင်ဖုန်းဆက်ပြီး (သို့မဟုတ်) သင့်ဘဏ်ဝက်ဘ်ဆိုက်ရဲ့ URL ကို ရိုက်ထည့်ပြီး အတည်ပြုချက်ရယူသင့်ပါတယ်။ အဲ့လိုပါပဲ သင့်ဦးလေးဘိုးရစ်က သင့်ကို ဖိုင်တဲ့တွဲထားတဲ့ အီးမေးလ်တစ်ခုပို့ရင်လည်း သူ့ဆီဖုန်းဆက်မေးပြီးမှ ဖွင့်သင့်ပါတယ်။

Google Drive ကိုသုံးပြီး သံသယဖြစ်ဖွယ်စာရွက်စာတမ်းများအား ဖွင့်ခြင်း

အလုပ်သဘောအရ တချို့လူတွေကျ ကိုယ်မသိတဲ့သူတွေဆီကနေဖိုင်တွေကို လက်ခံရလေ့ရှိပါတယ်။ ဥပမာ- သတင်းထောက်တွေဆို လူအမျိုးမျိုးဆီက သတင်းအမျိုးမျိုးပါဝင်တဲ့ စာရွက်စာတမ်းတွေကို

လက်ခံရပါတယ်။ Word ဖိုင်ဖြစ်စ်၊ Excel ဖိုင်ဖြစ်ဖြစ်၊ pdfဖြစ်ဖြစ် အဲဒီဖိုင်တွဲတွေထဲမှာ တိုက်ခိုက်မှုကို ဝှက်ပြီးထည့်ပေး၊ မပေးဆိုတာကို မျက်စိနဲ့ အလွယ်တကူအတည်ပြုဖို့မလွယ်ပါဘူး။

အဲ့လိုအခါမျိုးမှာ ဖိုင်ကို ကလစ်နှစ်ချက်နှိပ်ပြီးဖွင့်မယ့်အစား Google Drive (သို့မဟုတ်) အခြား အွန်လိုင်းကိုသုံးပြီး စာရွက်စာတမ်းတွေဖွင့်လို့ရတဲ့ reader ထဲ uploa လုပ်ပါ။ အဲ့ဒီလိုလုပ်လိုက်တာနဲ့ စာရွက်စာတမ်းကို ဓါတ်ပုံ (သို့မဟုတ်) HTML ပုံစံပြောင်းလိုက်တာမို့ သင့်စက်ပစ္စည်းထဲမှာ malware ကို ထည့်သွင်းလို့မရတော့ပါဘူး။ တကယ်လို့သင့်အနေနဲ့ ဖိုင်တွေ၊ အီးမေးလ်တွေဖွင့်တဲ့အခါ malware တိုက်ခိုက်မှုရဲ့ အကျိုးဆက်တွေ ကို ကန့်သတ်နိုင်တဲ့ စနစ်တစ်ခုကို အချိန်ပေးပြီး တပ်ဆင်အသုံးပြုဖို့စိတ်ဝင်စားရင်တော့ သုံးနိုင်တဲ့ ဆော့ဖ်ဝဲလ်တွေအကြောင်းရှင်းပြပါမယ်။ TAILS ဟာ Linux-based operating system လင်းနစ်ကို အခြေခံတဲ့ အော်ပရေးရှင်းစနစ်တစ်ခုဖြစ်ပြီး သင်အသုံးပြုပြီးတာနဲ့ ဖျက်ပေးပါတယ်။ နောက်ထပ် လင်းနစ်ကိုအခြေခံတဲ့ စနစ်တစ်ခုကတော့ Qubes ဖြစ်ပြီး အက်ပလီကေးရှင်းတစ်ခုနဲ့တစ်ခုအကြား အနှောင့်အယှက်မပေးနိုင်အောင် ကန့်ပေးထားလို့ malware ရဲ့ အကျိုးဆက်တွေကို ကန့်သတ်ပေးနိုင်ပါတယ်။ နှစ်မျိုးလုံးကို လက်ပ်တော့ရော၊ အထိုင်ကွန်ပျူတာတွေမှာပါ သုံးနိုင်ပါတယ်။

သင့်အနေနဲ့ Virus Total ကိုသုံးပြီး မယုံကြည်ရတဲ့ လင့်ခ်တွေကို ပို့ပြီးစစ်ဆေးနိုင်ပါတယ်။ Virus Total က ပို့လာတဲ့ဖိုင်တွေကို မတူညီတဲ့ antivirus အင်ဂျင်တွေသုံးပြီး စစ်ဆေးပေးပြီး ရလဒ်တွေကို အစီရင်ခံစာထုတ်ပေးပါတယ်။ ဒါကလည်း လုံးဝဥဿုံစိတ်ချရတာတော့မဟုတ်ပါဘူး။ အချို့ antivirus တွေက malware အသစ်တွေ (သို့မဟုတ်) ဦးတည်တိုက်ခိုက်မှုတွေကို မရှာဖွေပေးနိုင်ပါဘူး။ ဒါပေမဲ့လည်း ဘာမှမရှိတာထက်တော့ ကောင်းပါသေးတယ်။

တစ်ခုသတိပြုရမှာက လူအများဝင်သုံးလို့ရတဲ့ ဝက်ဘ်ဆိုက်တွေဖြစ်တဲ့ VirusTotal တို့ Google Drive တို့ကို အသုံးပြုမယ်ဆိုရင်၊ အဲဒီအထဲကို သင့်ကုမ္ပဏီကသူတွေ (သို့မဟုတ်) ဝင်ခွင့်ရှိတဲ့ အခြားသူတွေဝင်ကဝင်ရောက်ကြည့်ရှုနိုင်ပါတယ်။ ဖိုင်တွေက လူအများမကြည့်သင့်တဲ့ အကြောင်းအရာတွေ၊ လျှို့ဝှက်ဖိုင်တွေသာ ဖြစ်နေမယ်ဆိုရင်တော့ ဒီနည်းလမ်းကို ပြန်စဉ်းစားသင့်ပါတယ်။

ဘုံသုံးဒုတိယအတည်ပြုသော့ကို login အတွက် သုံးခြင်း

အချို့ဆိုက်တွေမှာ ဖစ်ရှင်းတိုက်ခိုက်မှုတွေကို ရှောင်လွှဲနိုင်ဖို့ တိုကင်စက်လေးတွေနဲ့ အသုံးပြုဖို့ ခွင့်ပြုပါတယ်။ အဲဒီတိုကင် (သော့ချောင်း) လေးတွေက သင့်ဘရောက်ဇာနဲ့ ဆိုက်တစ်ခုချင်းစီ အကြား login ဝင်တဲ့အချိန်မှာ ချိတ်ဆက်နိုင်တဲ့ pre-site credentialsကို ထုတ်ပေးပါတယ်။ အဲ့ဒါကိုဘုံသုံး ဒုတိယအတည်ပြုသော့ Universal 2nd Factor or “U2F,” လို့ခေါ်ပါတယ်။ ဘာလို့ အဲဒီလို ခေါ်လဲဆိုတော့ အဲဒီသော့က login မှာ သင်သုံးတဲ့စကားဝှက်ကို ထပ်ပေါင်းပြီး အသုံးပြုသူကို အတည်ပြုစစ်ဆေးတဲ့ ဒုတိယနည်းလမ်း အဖြစ် စံထားအသုံးပြုကြလို့ပါပဲ။ အသုံးပြုပုံက ရိုးရှင်းပါတယ်။ သင့်အနေနဲ့

ပုံမှန်နည်းလမ်းအတိုင်း login ဝင်တဲ့အချိန်မှာ သင့်သော့ကို သင့်ကွန်ပျူတာ (သို့မဟုတ်) စမတ်ဖုန်းမှာတပ်ဆင်ပြီး loginခလုတ်ကို နှိပ်ပါ။ တကယ်လို့ သင်က ဖစ်ရှင်းဆိုက်ကိုဖွင့်နေတာဆိုရင် တရားဝင်ဆိုက်နဲ့သာ ချိတ်ဆက်နိုင်တဲ့ credentials တွေကို အသုံးမပြုနိုင်လို့ ဘရောက်ဇာက သင့်ကို ဝင်ခွင့်ပြုမှာမဟုတ်ပါဘူး။ ဆိုလိုတာက သင့်ရဲ့စကားဝှက်ကို ဖစ်ရှင်းလုပ်သူတွေက လိမ်ယူဖို့ကြိုးစာတာဆိုရင် အထမမြောက်တော့ဘူးပေါ့။ Yibico (သော့ထုတ်လုပ်သူတစ်ဦး) က U2F နဲ့ပတ်သက်တဲ့ အချက်အလက်တွေကို ပြောပြထားပါတယ် more information about U2F။

ဒီနည်းလမ်းကို ဖစ်ရှင်းကာကွယ်မှု ပေးနိုင်ဖို့မသေချာတဲ့ ဒုတိယအကြိမ်အတည်ပြုစစ်ဆေးခြင်း နည်းလမ်းဖြစ်တဲ့ two-factor authentication နဲ့ မမှားသင့်ပါဘူး။

အီးမေးလ်းကပေးဖို့တဲ့ ညွှန်ကြားချက်တွေနဲ့ပတ်သက်လို့ သတိပြုပါ။

အချို့ဖစ်ရှင်းအီးမေးလ်တွေက ကွန်ပျူတာအထောက်အကူပြုဌာန (သို့မဟုတ်) နည်းပညာ ကုမ္ပဏီတစ်ခုခုက လာတဲ့ပုံစံလုပ်ပြီး သင့်ရဲ့ စကားဝှက်နဲ့ပန်ဖို့ အကြောင်းကြားတာ (သို့မဟုတ်) ကွန်ပျူတာပြင်ဆင်သူက သင့်် ကွန်ပျူတာကို အဝေးကနေဝင်ရောက်ခွင့်ပြုဖို့ (သို့မဟုတ်) သင့်စက်ပစ္စည်းမှာဖွင့်ထားတဲ့ လုံခြုံရေးစနစ်ကို ပိတ်ပေးဖို့ဆိုတာမျိုးတွေပါတတ်ပါတယ်။ ဒီလို အီးမေးလ်တွေမှာ ပြောထားတဲ့အတိုင်းဘာလို့လုပ်ဖို့ လိုကြောင်းကို စာတတန်ပေတတန်ရှင်းပြတာ မျိုးတွေ ပါပါတတ်ပါတယ်။ ဥပမာ-သင့် အီးမေးလ်ဘောက်စ်ကပြည့်နေလို့ (သို့မဟုတ်) သင့်ကွန်ပျူတာ အဟက်ခံရတယ်ဆိုတာမျိုးပေါ့။ သင်အနေနဲ့ ဒီလိုအီးမေးလ်တွေကို ယုံစားလိုက်ရင်တော့ လုံခြုံရေးကျိုးပေါက်ပြီသာမှတ်ပေတော့။ အထူးသဖြင့် သင့်အနေနဲ့ technical data နည်းပညာဆိုင်ရာအချက်အလက်တွေမပေးခင် (သို့မဟုတ်) နည်းပညာ ညွှန်ကြားချက်တွေ အတိုင်း မလုပ်ခင်မှာ စာက အမှန်အကန်ဖြစ်ကြောင်း အတည်ပြုချက်အရင်ရယူသသင့်ပါတယ်။

တကယ်လို့သင့်ဆီသံသယဖြစ်ဖွယ် အီးမေးလ် (သို့မဟုတ်) လင့်ခ်တစ်ခုကို တစုံတယောက်က ပေးဖို့လိုက်တယ်လို့ထင်ရင် အထက်မှာဖော်ပြခဲ့တဲ့ လုံခြုံရေးအစီအမံတွေ၊ အကြံပြုချက်တွေကို မလုပ်ဘဲ ဒါမဟုတ် အဲဒါက တိုက်ခိုက်မှုမဟုတ်ကြောင်း မသေချာဘဲ မဖွင့်ပါနဲ့(သို့) ကလစ်မနှိပ်မိပါစေနဲ့။