Security Alert

Facebook Scam တွေကို သတိပြုရောင်ရှားပါ

တချို့ လိမ်လည်မှုတွေအကြောင်းကို ကြားဖူးမှာ ဖြစ်ပြီး ကိုယ်တိုင်လည်း ဖျားယောင်းခံရဖူးမှာပါ။ ဒီမှာတော့ နောက်တစ်ကြိမ် သားကောင်အဖြစ်မခံရစေဖို့ နည်းလမ်းတွေကို တင်ပြလိုက်ပါတယ်။

"မိနစ်တိုင်းမှာ လိမ်ညာခံရတဲ့လူတစ်ယောက် ပေါ်ပေါက်နေပါတယ်" ဆိုတဲ့ အဆိုက မူလက carnival ပွဲတော် (ဆပ်ကပ်) ကြည့်တဲ့သူတွေအတွက် P.T.Barnum က ညွှန်းဆိုပြောကြားခဲ့တာဖြစ်ပါတယ်။ ဒါပေမဲ့ ဒါက ဒီနေ့ခေတ် online scam တွေနဲ့လည်း ကိုက်ညီနေပါတယ်။ အထူးသဖြင့် facebook scam တွေနဲ့ ကိုက်ညီနေပါတယ်။

ဥပမာ – facebook အယောင်ဆောင်တွေဖြစ်တဲ့ facebook dislike button ၊ ကိုယ့် profile ကို ဘယ်သူတွေ လည်ပတ်သွားတယ်ဆိုတာပြောမယ့် stalker tracker နဲ့ "watch this video" လှည့်ကွက်တွေက အသစ်အဆန်းတွေ မဟုတ်ကြပါဘူးလို့ အင်္ဂလန်အခြေစိုက် GFI software ရဲ့ အကြီးတန်း threat researcher Chris Boyd က ဆိုပါတယ်။ လူတွေက ဒီ လှည့်ကွက်တွေထဲ မရောက်တော့ဘူးလို့ ထင်မိမှာပါ။ ဒါပေမဲ့ သူတို့က အညာခံနေရတုန်းပါပဲ။ Click လုပ်ဖို့ ဆွဲဆောင်ထားတာကို ငြင်းဆန်ရတာ ခက်ခဲပါတယ်။ Scammer တွေကလည်း အဲဒါကိုသိပါတယ်။

သူတို့က သုံးစွဲသူတွေရဲ့ စပ်စုတဲ့စိတ်၊ ယုံကြည်မှုနဲ့ သူတို့ရဲ့ အမှန်ပုံစံမျိုး လိမ်ညာဟန်ဆောင်နိုင်စွမ်းတွေကို ပေါင်းစပ်အသုံးချကြတာပဲ ဖြစ်ပါတယ်။ ကံကောင်းတာက အဲဒါတွေကို စောင့်ကြည့်နိုင်တဲ့ သဲလွန်စအချို့ ရှိနေပါတယ်။

မိတ်ဆွေအတုအယောင်များ

Facebook scammer တွေသုံးတဲ့ လှည့်ကွက်တစ်ခုကတော့ ဆွဲဆောင်မှုရှိတဲ့ URL တွေကို click နှိပ်ဖို့ လူတွေကို တိုက်တွန်းထားတာပါပဲ။ ဒါပေမဲ့ နှိပ်လိုက်ရင် သူပြောတဲ့ site ကိုမရောက်ဘဲ ကိုယ့်မိတ်ဆွေတွေဆီကို အဲဒီ URL ကိုပဲ spam ပို့ မိသားဖြစ်သွားမှာပါ။ တချို့ဖော်ပြချက်တွေက တကယ်လက်ခံယုံကြည်နိုင်လောက်လို့ အလိမ်ခံရတဲ့သူက အကြွေးဝယ် card နံပါတ်တွေ၊ phone နံပါတ်တွေလိုမျိုး အချက်အလက်တွေ ပေးမိနိုင်ပါတယ်။ ဒီအချက်အလက်ကိုသုံးပြီး scammer တွေက တရားမဝင် ငွေချေမှုတွေကို ပြုလုပ်နိုင်ပါတယ်။

Scam လုပ်တာအောင်မြင်ဖို့ အဓိကအချက်က အလိမ်ခံရ

မယ့်သူရဲ့ ယုံကြည်မှုကို ရယူနိုင်စွမ်းပဲဖြစ်ပါတယ်လို့ Philadelphia က Drexel University ရဲ့ လူမှုဌာနက တွဲဖက်ပါမောက္ခ Dr.Robert D'Ovidio က ဆိုပါတယ်။ Scam အများစုက ကိုယ်သိတဲ့သူတွေရဲ့ post တွေထဲက link တွေ ပုံစံမျိုးဟန်ဆောင်ထားကြပါတယ်။ ဒီအစီအစဉ်တွေက user တွေရဲ့ ကွန်ရက်ထဲက လူတွေဆီက လာတာပါ။ ဒါကြောင့် ဒါက ရင်ဆိုင်ရ အတော်ခက်ခဲပါတယ်။

တကယ်လို့ ကိုယ့်မိတ်ဆွေတစ်ယောက်က video မှာ ဘာရှိသလဲဆိုပြီး ကိုယ့်ဆီမှာ link ကို post တင်သွားပြီး "အဲဒါ မင်းလား" လို့ comment ပေးထားရင် ကိုယ်က click လုပ်မိနိုင်ပါတယ်။ ဒါပေမဲ့ ဒါက scam ၊ ဒါမှမဟုတ် hijacked အလုပ်ခံထားရတဲ့ facebook account ကိုသုံးပြီး malicious site ဆီကို ညွှန်းထားတဲ့ link ဖြစ်နိုင်ပါတယ်။

Link တစ်ခုကို click နှိပ်မိတဲ့အခါ ကိုယ်သတိပြု စောင့်ကြည့်ရမယ့် အချက် ၂ ချက်ရှိပါတယ်။ အဲဒါတွေကတော့ သူညွှန်းထားတဲ့ page ဆီ မရောက်သွားတာနဲ့ ကိုယ် မျှော်လင့်ထားတာထက် အရမ်းကြာနေတာတို့ပါပဲ။ အဲဒီလို ကြာနေရတဲ့ အကြောင်းက hacker ရဲ့ တည်နေရာကို မသိစေချင်လို့ ညွှန်းထားတဲ့ page ကို တိုက်ရိုက်ပို့ရမယ့်အစား proxy server တွေကြား ဗျာများခိုင်းထားတာပါ။

ဒါ့အပြင် ကိုယ့်ရဲ့ facebook login အချက်အလက်တွေကို အမှတ်မထင်မေးတတ်တဲ့ page တွေကိုလည်း သတိထားစောင့်ကြည့်ပါ။ Scammer တွေက ကိုယ့် account အသေးစိတ် အချက်အလက်တွေကိုရရှိဖို့ စီမံပြီးတာနဲ့ အဲဒါကိုသုံးပြီး ကိုယ့်သူငယ်ချင်းတွေဆီကို spam လုပ်နိုင်ပါတယ်။ အဲဒီလို ဖြစ်သွားခဲ့ရင်၊ ဒါမှမဟုတ် ဖြစ်နေတယ်လို့ သံသယရှိရင် password ကို ချက်ချင်းပြောင်းပစ်ပါ။

Shortened URL (အတိုကောက်လိပ်စာ) တွေတောင်မှ အန္တရာယ်ရှိနိုင်ပါတယ်။ ဘာဖြစ်လို့လဲဆိုတော့ သုံးစွဲသူတွေက အတိုကောက် web address တွေကိုကြည့်ပြီး ဒါက အစစ်အမှန်ဟုတ်ရဲ့လားဆိုတာ မပြောနိုင်လို့ပါပဲ။ ဒါ့ကြောင့် တစ်ယောက်ယောက်က ကိုယ့် စာမျက်နှာပေါ်မှာ၊ ဒါမှမဟုတ် facebook message ၊ ဒါမှမဟုတ် chat နဲ့ အတိုကောက်လိပ်စာတစ်ခု ပို့လိုက်တယ်ဆိုရင် သတိနဲ့ လုပ်ဆောင်ပါ။

နောက်ပိုင်းမှာ scam အများစုကို pay-per-click တွေကနေ scammer တွေဆီ ပိုက်ဆံရောက်အောင်၊ ဒါမှမဟုတ် အကြွေးကဒ် ၊ phone bill တွေကနေ တရားမဝင်ငွေပေးချေမှုတွေ လုပ်နိုင်တဲ့ အချက်အလက်တွေရရှိအောင် design လုပ်ထားကြပါတယ်။

လှည့်ကွက်မိသွားရင် ဘာလုပ်ရမလဲ

ကိုယ် scam အလုပ်ခံလိုက်ရပြီဆိုရင် ပထမဆုံး အနှောင့်အယှက်ပေးနေတဲ့ app ကို delete လုပ်ပါ။ Account>> privacy setting>>edit your setting ထဲက "app and website အောက်ထဲဝင်ပြီး ကိုယ်သုံးတဲ့ app တွေရဲ့ edit setting ထဲဝင်ပြီး ဖျက်ချင်တဲ့ app ရဲ့နားက 'X' ကို နှိပ်ပါ။ ပြီးတော့ app က ကိုယ့်နာမည်နဲ့ဖန်တီးခဲ့တဲ့ post တွေ အားလုံးကို ဖျက်ပစ်ပါ။ ပြီးတော့ ကိုယ့်သူငယ်ချင်းတွေကို ဖြစ်ပျက်သွားတာတွေပြောပြပြီး facebook account password ကိုပြောင်းပါ။

Scam အလုပ်မခံရဖို့ အဓိကနည်းလမ်းကတော့ အာရုံစိုက်သတိထားဖို့ပါပဲ။ Privacy setting တွေ အားလုံးကို တင်းကျပ်ထားဖို့နဲ့ app တွေက ကိုယ့်ရဲ့ အချက်အလက်တွေ၊ facebook page တွေနဲ့ ပတ်သက်ပြီး လုပ်ကိုင်နိုင်တာတွေကို ကန့်သတ်ထားဖို့ လိုပါတယ်။ ဒီ setting တွေ ပြင်ဆင်ဖို့ facebook ထဲ log in ဝင်ပြီး ညာဘက်ထောင့် account ဆိုတာကို click နှိပ်ပါ။ ပြီးတော့ ဘယ်ဘက်အောက်ခြေက app and website အောက်မှာရှိတဲ့ edit your setting ဆိုတာ ကိုရွေးပြီး info accessible through your friend နားက edit setting ဆိုတာ ကိုနှိပ်ပါ။

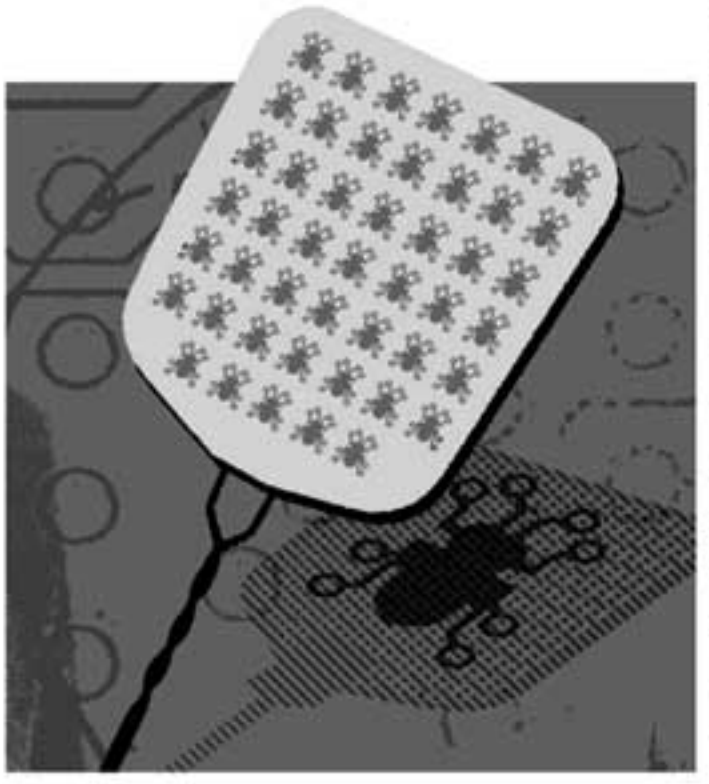
ယုံကြည်မှုမလွန်ကဲတာက ကောင်းတဲ့အချက်ပါ။ အောက်မှာ အကြံပြုချက်လေးတွေ ဖော်ပြပေးလိုက်ပါတယ်။

- App author ကို စစ်ဆေးပါ။ Author ရဲ့ နာမည်ပေါ် click နှိပ်ပြီး app ရဲ့ homepage ကိုကြည့်ပါ။ ထူးဆန်းတာ၊ ပုံမှန်မဟုတ်တာတွေကိုရှာပါ။ App ရဲ့ နာမည်နဲ့ author ကို google မှာ ရှာဖွေမှုလုပ်ကြည့်ပါ။
- အခြားအသုံးပြုသူတွေရဲ့ အတွေ့အကြုံကိုလည်း လေ့လာပါ။ ရိုးရှင်းတဲ့ ရှာဖွေမှုတစ်ခုက အစစ်အမှန် ဟုတ်၊ မဟုတ် ပြောပြနိုင်မှာပါ။
- Facebook log in name နဲ့ password အပါအဝင် ကိုယ်ရေးကိုယ်တာအချက်တွေကို လက်ခံမယ့်သူက တရားဝင်မဟုတ်ဘူးလို့ သုံသယရှိ၊ မရှိ မသေချာရင် မပေးပါနဲ့။
- ကိုယ့်ရဲ့ လူမှုကွန်ရက်ပေါ်က လုံခြုံရေးက ကိုယ့်ကွန်ရက်ထဲမှာရှိတဲ့လူတွေရဲ့ လုံခြုံရေးသတိကင်းမဲ့မှုအပေါ်မှာလည်း တစ်စိတ်တစ်ဒေသ မူတည်နေတယ်ဆိုတာကို မမေ့ပါနဲ့။
- ဒါက ဒုံးကျည်သိပ္ပံပညာရပ်လိုမျိုး ခက်ခဲတဲ့ကိစ္စတွေ မဟုတ်ပါဘူး။ ဒါပေမဲ့ လုံခြုံရေးကျွမ်းကျင်သူတွေကတော့ ကိုယ် click လုပ်မယ့်အရာကို ဂရုစိုက်တာ အကောင်းဆုံးပဲလို့ ဆိုကြပါတယ်။

Bugs & Fixes

Google က chrome browser အတွက် ပြင်ဆင်ချက်တွေ ထုတ်ပေးခဲ့ပါတယ်။ ဒါ့အပြင် Mac 5 အတွက် Skype update တစ်ခု ထွက်ခဲ့ပြီး OSX malware monitoring မှာ လည်း ပြောင်းလဲမှုတစ်ခု လုပ်ပေးခဲ့ပါတယ်။

မကြာသေးမီက တွေ့ရှိခဲ့တဲ့ bug တွေကြောင့် google က chrome browser အတွက် ပြင်ဆင်မှုအများအပြား ထုတ်ပေးခဲ့ပါတယ်။ Skype ကလည်း Skype 5 for Mac အတွက် အလွန်အန္တရာယ်ကြီးတဲ့ ယိုပေါက်ကို ပြင်ဆင်ချက်ထုတ်ပေးခဲ့ပါတယ်။ တိုက်ခိုက်သူတွေက အဲဒီဟာကွက်ကတစ်ဆင့် system အပေါ် အပြည့်အဝ ထိန်းချုပ်မှုလုပ်သွားစေနိုင်ပါတယ်။ Apple ကလည်း ဗီဇပြောင်းလွယ်တဲ့ Mac Defender scareware ကို တုံ့ပြန်တဲ့ အနေနဲ့ Mac OSX function ထဲက malicious-file quarantine system နည်းလမ်းကို ပြောင်းလဲခဲ့ပါတယ်။



လုံခြုံရေးအဖွဲ့တစ်ခုဖြစ်တဲ့ Vupen က တိုက်ခိုက်သူတွေက google chrome ရဲ့ sandbox ကို ကျော်ပြီး အန္တရာယ်များတဲ့ code တွေကို ကိုယ့်စနစ်ပေါ်မှာ run ခွင့်ပြုနိုင်တဲ့ bug ကို မကြာသေးမီက ရှာတွေ့ခဲ့တာပဲ ဖြစ်ပါတယ်။ Google ကတော့ ဒီ bug run ဖို့ flash လိုအပ်တာကြောင့် ဒါက အခြေခံအားဖြင့်တော့ Adobe ရဲ့ bug ပါလို့ ဆိုပါတယ်။ Google ရဲ့ နောက် ဆုံး update က ဒီပြဿနာကို Adobe ရဲ့ flash player version 10.2 ကို install လုပ်ပြီး ဖြေရှင်းပေးလိုက်တာပါ။

Chrome ကတော့ browser version အသစ်ထွက်တယ်ဆိုရင် အလိုအလျောက် update လုပ်ဖို့ စီစဉ်ထားပါတယ်။ ဒါပေမဲ့ အကြောင်းတစ်ခုခုကြောင့် browser update မဖြစ်ဘူးဆိုရင် toolbar ထဲက ဝွရှင်ပုံစံလေးကို click နှိပ်ပြီး update google chrome ကိုရွေးပါ။ ဒီ update တွေနဲ့ပတ်သက်ပြီး ပိုသိချင်တယ်ဆိုရင်တော့ *(find.pcworld.com/71902)* မှာ ကြည့်နိုင်ပါတယ်။

Mac user များအတွက် update

မကြာသေးမီကတွေ့ရှိခဲ့တဲ့ Skype 5 for Mac မှာရှိတဲ့ လုံခြုံရေးယိုပေါက်က တိုက်ခိုက်သူတွေက အထူးစီစဉ်ထားတဲ့ message တစ်ခုကို ပို့လိုက်ရင် Skype ကို crash ဖြစ်စေပါတယ်။ ဒီယိုပေါက်ဟာ application ရဲ့ interface feature တစ်ခုကနေ remote control လုပ်သွားနိုင်ပါတယ်။ Skype ကတော့ ဒီယိုပေါက်က တိုက်ခိုက်မခံရသေးဘူးလို့ ဆိုပါတယ်။

ဒါပေမဲ့ ဘာတိုက်ခိုက်မှမှ မဖြစ်စေချင်တဲ့အတွက် Skype for Mac နောက်ဆုံး version (5.1.0. 922 နဲ့ အထက်)ကို update လုပ်ဖို့တိုက်တွန်းထားပါတယ်။ ဒါ့ပြင် Skype က bug တစ်ခုက user တွေကို log on လုပ်ရာမှာ တားဆီးမှု ကြံ့အပြီးမှာတော့ Windows အတွက်နဲ့ Mac အတွက် သီးခြား update ၂ ခုကို ထုတ်ပေးခဲ့ပါတယ်။

Mac သုံးစွဲသူတွေကတော့ security update 2011-003 for Mac OSX snow leopard ကိုပါ install လုပ်သင့်ပါတယ်။ ဒီ patch က အခုတလောမှာတွေ့ရှိခဲ့တဲ့ MacDefender antivirus အတုလိမ်လို malware အသစ်တွေကို သိရှိနိုင်ဖို့ definition update အသစ်တွေကို နေ့စဉ်စစ်ဆေးဖို့ Mac OSX က malicious file quaranfine စနစ်ကို ပြင်ဆင်ပေးပါတယ်။ Update ဖြစ်နေတာသေချာစေဖို့ software update ကို Mac ပေါ်မှာ run ပါ။ အချက်အလက်တွေ ပိုမိုသိချင်ရင်တော့ *(find.pcworld.com/71916)* မှာ ဖတ်ရှုနိုင်ပါတယ်။

West Hero