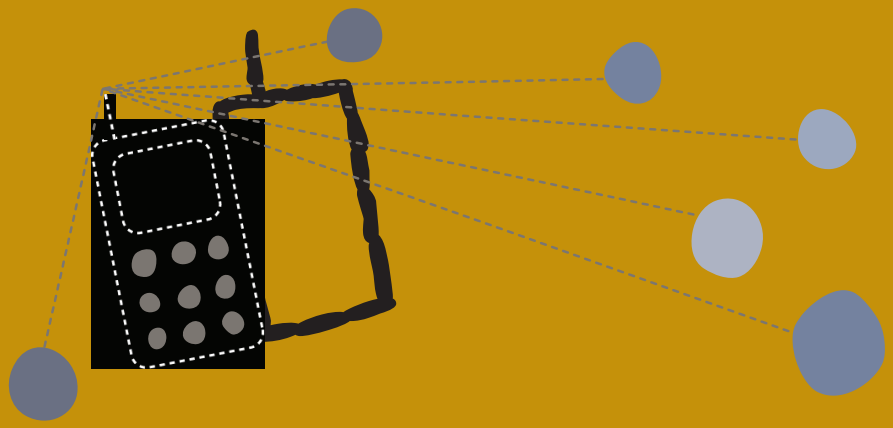
အွန်လိုင်း၊ လက်ကိုင်ဖုန်းလုံခြုံရေးနဲ့ အတွင်းရေး



ဆန်းသစ်လာတဲ့ နည်းပညာများ၊ အထူးသဖြင့် မိုဘိုင်းဖုန်းများနဲ့ အင်တာနက်ဟာ ဂါဒဖြန့်ရေးအတွက် အစွမ်းထက်တဲ့ အထောက်အကူတွေဖြစ်လာပါတယ်။ ဒါပေမဲ့လည်း ဒီလိုပစ္စည်းတွေသုံးပြီး အရေးကြီးတဲ့ အချက်အလက်တွေဖြန့်ဖြူးရာမှာ ကိုယ်တိုင်နဲ့ မိတ်ဆွေလုပ်ဖော်ကိုင်ဖက်တွေအတွက် အန္တရာယ်ဖြစ်နိုင်တာမျိုးတွေ ရှိပါတယ်။ ဒါကြောင့် လက်ကိုင်ဖုန်းနဲ့ အင်တာနက်တွေသုံးပြီး ဘယ်လို လုံခြုံစွာအချက်အလက်ဖြန့်ဖြူးလို့ရတယ်၊ ကိုယ့်သတင်းအချက်အလက်တွေကို ကာကွယ်ပေးလို့ရတယ်ဆိုတာ သိအောင် ဒီကဒ်က ကူညီပါတယ်။

ဒစ်ဂျစ်တယ်လုံခြုံရေးနဲ့ ထိန်းသိမ်းလျှို့ဝှက်ခြင်း ဆိုတာ ဘာလဲ။
အချက်အလက်ရယူခွင့်နဲ့ ဒစ်ဂျစ်တယ်လုံခြုံရေးနဲ့ ပတ်သက်ပြီး သတိထားစရာအချက်များကတော့

- ကိုယ်မသိလိုက်ပဲ Password ပြောင်းသွားခြင်း
- နှစ်ကိုယ်ကြားသိရမယ့် သတင်းစကားများကို လက်ခံရမည့်သူမဟုတ်သော တစုံတယောက်က ဖတ်ထားခြင်း
- နိုင်ငံအချို့မှ ကြည့်မရဖြစ်လာတဲ့ ဝက်ဆိုဒ်များ
- လျှို့ဝှက်သင့်တဲ့ ဆက်သွယ်ရန်လိပ်စာများ၊ နေ့စွဲများ၊ အမည်များနဲ့ ဆွေးနွေးထားတဲ့ အကြောင်းအရာတွေကို လိုက်ဖော်ထုတ်ဖို့ကြိုးစားနေတဲ့ အရာရှိများ
- လက်ကိုင်ဖုန်းပေါ်မှ စကားအသွားအလာတွေကို တောက်လျှောက်စောင့်ကြည့်ခံနေရတယ်လို့ သံသယရှိလာခြင်း

ဒီကိစ္စများနဲ့ပတ်သက်ပြီး စိုးရိမ်ရပါမလား။
စီမံကိန်း ဒါမှမဟုတ် ကိုယ်တိုင် သို့မဟုတ် အဆက်အသွယ်တွေနဲ့ ပတ်သက်ပြီး ဖော်ပြပါ အခြေအနေမျိုး ဖြစ်လာမယ်ဆိုရင်တော့ စိုးရိမ်စရာရှိပါတယ်။ ဒစ်ဂျစ်တယ်လုံခြုံရေးကို ထိခိုက်အောင်လုပ်နိုင်တဲ့ software တွေနဲ့ ဘယ်လိုလုပ်လို့ရတယ်ဆိုတဲ့ အကြောင်းတွေကို အင်တာနက်ပေါ်မှာ ရှာရနိုင်ပါတယ်။ တကယ်လို့ တိုက်ခိုက်လိုသူက အင်တာနက်အသုံးပြုခွင့်ကောင်းကောင်း ရှိနေမယ်၊ နိုင်ငံတွင်း မိုဘိုင်းဖုန်းများ အလုပ်လုပ်ပုံ အခြေခံစနစ်ကို သိနေမယ် ဆိုရင် သူအတွက် ဒါဟာ အရမ်းလွယ်တဲ့ ကိစ္စဖြစ်သွားပါပြီ။ အစိုးရအဖွဲ့အစည်းတွေ၊ အင်တာနက်ဝန်ဆောင်မှုပေးသူတွေ (ISPs) နှင့်

မိုဘိုင်းဖုန်းကုမ္ပဏီများဟာ ဒီလိုအခြေခံစနစ်များထဲ ဂင်ရောက်သိရှိခွင့်ရှိပါတယ်။ ဒါ့အပြင် ရုံးကလုပ်ဖော်ကိုင်ဖက်များ၊ အိမ်နီးချင်းများနဲ့ အင်တာနက်ဆိုင်များက စက်ပိုင်းဆိုင်ရာစီမံခန့်ခွဲသူများမှာလည်း ဂင်ရောက်နိုင်ခွင့်အနည်းအကျဉ်းရှိပါတယ်။

ဘယ်လိုလုံခြုံရေး အရေးကိစ္စများကြောင်း ဒီကဒ်မှာ ရှင်းပြထားပါသလဲ။

ကွန်ယက်အခြေပြုအသုံးချကိရိယာများနဲ့ မိုဘိုင်းဖုန်းများအကြောင်းကို အဓိကထားရှင်းပြထားပါတယ်။ သို့သော် စိစစ်ရေးနဲ့ပြဿနာတွဲ့၊ စောင့်ကြည့်ခံရနိုင်တဲ့၊ ဖိနှိပ်ခံရခြင်းများ ရှိနိုင်တဲ့ တခြားနည်းပညာများလည်း ရှိပါသေးတယ်။ ထိုအကြောင်းအရာများနှင့် ပတ်သက်ပြီး ဒီနေရာမှာ ဆွေးနွေးထားခြင်း မရှိပေမယ့်လည်း ကွန်ပျူတာစနစ်ကို ပုံမှန်မွမ်းမံအဆင့်မြှင့်ခြင်း၊ စိတ်ချရတဲ့ anti-malware ဆော့ဖ်ဝဲများ ထည့်သွင်းခြင်းများနဲ့ Back-up များမပြတ်ထားရှိခြင်းစတဲ့ လုပ်ဆောင်ချက်များဟာ အရေးပါတဲ့အခြေခံ ကြိုတင်ကာကွယ်ခြင်းမျိုးဖြစ်ပါတယ်။ ကွန်ပျူတာတွေ သို့မဟုတ် Back-up တွေ အပါအဝင် အချက်အလက်သိမ်းဆည်းထားတဲ့ ကိရိယာတွေ ပျောက်ဆုံးနိုင်တယ်၊ အခိုးခံရနိုင်တယ် သို့မဟုတ် အသိမ်းခံရနိုင်တယ် သို့မဟုတ် အဖွဲ့အစည်းဟာ အင်တာနက်ပေါ်မှာ အဓိကစောင့်ကြည့်ခြင်းခံနေရနိုင်တယ်လို့ ထင်တယ်ဆိုရင် Tactical Tech က လုပ်ထားတဲ့ Security in-a-Box Toolkit ကို ညွှန်းသင့်ပါတယ်။

ထွောက်ခံအားပေးရန်အတွက် အသုံးပြုသော ကွန်ယက်အခြေပြု Tool များ

ယုံကြည်အားကိုးရလောက်တဲ့ ကွန်ရက်အခြေပြု စည်းရုံးရေးအတွက် သို့မဟုတ် ညှိနှိုင်းဆောင်ရွက်မှုများအတွက် ဒီဘလော့များ၊ Twitter နဲ့ Facebook လို အများသုံးကွန်ယက်အခြေပြုကြားခံများကို သုံးမယ်ဆိုရင်တော့ သိလောင်ထားတဲ့ အချက်အလက်တွေ အားလုံး ယင်းတို့ အသုံးပြု ပလက်ဖောင်းများပေါ် ရောက်နေမှာဖြစ်ပြီး ထင်တာထက် ပေါက်ကြားဖို့ ပိုလွယ်ပါတယ်။

အလွန်သတိထားရမယ့် အရေးကိစ္စများအတွက် အွန်လိုင်းကိုသုံးရတော့မယ်ဆိုရင် သုံးစွဲသူကိုကာကွယ်ပေးမယ့် မူဝါဒတွေ သို့မဟုတ် သုံးစွဲသူသဘောတူညီချက် စတာတွေကို သေချာအောင်ဖတ်ဖို့ လိုပါတယ်။ အဆင့်အမြင့်ဆုံးဆိုတဲ့ မူဝါဒကတောင် ခွင့်ပြုချက်မပါပဲ မသိလိုက်ပဲ အချက်အလက်တွေကို ပေါက်ကြားစေနိုင်ခြင်း၊ ရောင်းချနိုင်ခြင်း သို့မဟုတ် အထားမှားခြင်းစတာတွေလုပ်နိုင်ချေရှိတဲ့ သက်ဆိုင်ရာပလက်ဖောင်းတွေကို ချုပ်ကိုင်သူတွေရဲ့လက်အောက်ရောက်သွားခြင်းကို မတားနိုင်ပါဘူး။ အကောင့်ကို လုံးဝရပ်စဲလိုက်မယ်ဆိုရင်တောင်မှ ဒီလို ဂဘ်ဆိုဒ်တော်တော်များများက ပေးထားပြီးသား အကြောင်းအရာတွေနဲ့ ကိုယ်ရေးကိုယ်တာတွေကို ဖျက်ပစ်တာမျိုးမရှိပါဘူး။ နောက်ဆုံး အောက်ခြေကလူထုနဲ့ထိတွေ့ချင်လို့ပဲဖြစ်ဖြစ်၊ သုံးရလွယ်လို့ပဲဖြစ်ဖြစ် စီးပွားဖြစ်ဂန်ဆောင်မှုတခုကို မသုံးမနေရသုံးရတာကလွဲရင် တခြားစိတ်ချရတဲ့ဂန်ဆောင်မှုမျိုး - ဥပမာ youtube အစား blip.tv၊ Gmail အစား riseup.net ဆိုတာမျိုးကို သုံးဖို့စဉ်းစားပါ။ ကိုယ်ပိုင်နည်းပညာများ သုံးစရာရှိတယ်ဆိုရင် ကိုယ်ပိုင်ကွန်ယက်အခြေပြု ဂန်ဆောင်မှုတခုလုပ်လိုက်ပါ။

စီးပွားဖြစ် ပလက်ဖောင်းတွေကို သုံးရတော့မယ်ဆိုရင် ဒီလိုအွန်လိုင်းပေါ် ကနေ သူတပါး သတင်းအချက်အလက်များကို မရအရရှာဖွေယူတတ်သူများဆီကကာကွယ်ဖို့ ကြိုတင်ကာကွယ်မှုများ လုပ်ထားပါ။ အထူးသဖြင့် လူထုဆက်သွယ်ရေးကွန်ယက်ဖြစ်တဲ့ Facebook တို့ Twitter တို့လို့ ဝက်ဆိုဒ်များဆို ပိုလိုပါတယ်။ ကိုယ် သို့မဟုတ် အဖွဲ့အစည်းနဲ့ ပတ်သက်ပြီး အရေးကြီးတဲ့ အချက်အလက်များ မရည်ရွယ်ပဲ ပေါက်ကြားသွားတာမျိုးက ကင်းဝေးအောင် ဒီပလက်ဖောင်းတွေမှာ ထည့်သွင်းရေးဆွဲထားတဲ့ အချက်အလက်လုံခြုံရေး နဲ့ ပတ်သက်သမျှကို နှုန့်နှစ်ပစ်ပ နားလည်အောင် လေ့လာထားပါ။ ဥပမာ - အမည်မှန်၊ နေရာလိပ်စာအမှန်၊ သွားရန်စီစဉ်ထားတဲ့ ခရီးနဲ့ စီစဉ်ထားတဲ့ အစည်းအဝေး သို့မဟုတ် အခမ်းအနားစတဲ့ အချက်အလက်တွေကို အချိန်ယူစောင့်ကြည့်ပြီး ကိုယ့်အကြောင်းနဲ့ အလုပ်လုပ်ပုံတွေကို ပုံဖော်လို့ရပါတယ်။

နည်းလမ်းကောင်းတခုရထားရုံနဲ့ အသုံးပြုနေတဲ့ ကွန်ယက်အခြေပြု ဂန်ဆောင်မှုတခုထဲမှာပဲ စီမံကိန်း အမျိုးမျိုးအတွက် တခုထက်မနည်းတဲ့အကောင့်များ ဖန်တီးနိုင်ခြင်း၊ ကိုယ်ရေးအကျဉ်းအမျိုးမျိုး သုံးနိုင်ခြင်းများအပြင် ကိုယ့်ကိုယ်ကိုယ် အပြင်လူအနေနဲ့ ထောက်လှမ်းကြည့်နိုင်တဲ့ အစမ်းအကောင့်များလည်း ထိန်းသိမ်းထားနိုင်ပါတယ်။ လုံခြုံရေးကို အကောင်းဆုံးကာကွယ်ပေးနိုင် တာကတော့ အကောင့်နဲ့ပတ်သက်ပြီး ဘယ်လိုရှာဖွေလို့ရတယ်ဆိုတာကို နည်းလမ်းပေါင်းစုံနဲ့ စမ်းကြည့်ခြင်းပါပဲ။ ဥပမာ - အွန်လိုင်း သို့မဟုတ် အချက်အလက်ကို ထိန်းသိမ်းထားတဲ့ အထူးပုဂ္ဂိုလ်များကတဆင့်

Password များ။

ကွန်ယက်အခြေပြုတဲ့ အရင်းအမြစ်တော်တော်များများမှာ အကောင့်ကို ကာကွယ်ပေးရန် Password တစ်ခုတည်းပေါ်မှာပဲ မူတည်ပါတယ်။ မလိုမုန်းထားသူ တဦး သို့မဟုတ် အဖွဲ့အစည်းများက ဒီPasswordကို သိသွားပြီဆိုပါက ဘယ်လောက်ပဲ အကောင့်ကိုင်တွယ်သူကို ယုံတာဖြစ်စေ သို့မဟုတ် လုံခြုံရေးစွမ်းပကားကို ဘယ်လောက် စမ်းသပ်ထားတာဖြစ်စေ အထူးလျှို့ဝှက်အတွင်းသတင်းများနဲ့ အမည်ဝှက်များကိုတော့ ဆုံးသွားပါပြီ။

လူသိနည်းတဲ့ Password ဖော်နည်းများကတော့ တယောက်ယောက်ကနေ လုံခြုံတဲ့ ဂဘ်ဆိုဒ် များဆီ Log in ဂင်တဲ့ ကွန်ပျူတာထဲကို Malware ဆော့ဖ်ဝဲထည့်သွင်းလို

က်ခြင်းမျိုးပါ။ သို့မဟုတ် မလုံခြုံတဲ့ ဖာ်ဆိုဒ်များ ဖင်နေစဉ် အင်တာနက်သုံးတာကို စောင့်ကြည့်တာမျိုး။

ပထမတိုက်ခိုက်ခံရမှုမျိုးက ကင်းဝေးချင်တယ်ဆိုရင်တော့ အမြဲတစေ ကိုယ်ပိုင်ကွန်ပျူတာ သို့မဟုတ် ယုံကြည်စိတ်ချရသူရဲ့ ကွန်ပျူတာကိုပဲ အသုံးပြုပါ။ ဒါ့အပြင် အသုံးပြုနေတဲ့ Operating System (ဥပမာ Window) နဲ့ Anti-Malware software များကို အမြဲတမ်း update လုပ်ပါ။ ဒုတိယတိုက်ခိုက်ခံရမှုက ကင်းဝေးလိုတယ်ဆိုရင်တော့ လူသိများတဲ့ ကွန်ယက်အခြေပြုအီးမေးလ်တွေ၊ လူမှုဆက်ဆံရေးအတွက် ကွန်ယက်တွေ၊ ဘလော့ဖန်တီးခြင်းတွေ၊ အမှတ်အသားပြုခြင်းတွေနဲ့ ဗီဒီယိုတွေအတွက် အသုံးပြုတဲ့ ပလက်ဖောင်းတွေက လုံခြုံရေးအတွက်ပေးတဲ့ ချိတ်ဆက်မှု HTTPS ကို သုံးနိုင်တယ်။ ဂင်ကြည့်နေတဲ့ ဖာ်ဆိုဒ်မှာ လုံခြုံတဲ့အင်တာနက်ချိတ်ဆက်မှုရှိမရှိသိချင်ရင် address bar ထဲမှာ ရှိတဲ့ ဖာ်ဆိုဒ်လိပ်စာဟာ 'https://' ဟုတ်မဟုတ်စစ်ကြည့်ပါ။ သူတို့ ဖာ်ဆိုဒ်ပေါ်က Password ကို ကာကွယ်ဖို့အတွက်ကလွဲလို့ သတင်းအချက်အလက်တွေကို https က ကာကွယ်မပေးပါဘူး။ ရလဒ်အနေနဲ့ အင်တာနက်ကော်နက်ရှင်ကို အချိန်အတိုင်းအတာတခုထိ စောင့်ကြည့်ရုံနဲ့ ထိုဆိုဒ်ပေါ်မှာ သိမ်းဆည်းထားသမျှကို သိသွားနိုင်ပါတယ်။ အကောင်းဆုံးရလဒ်ရှိတဲ့ ဖြေရှင်းနည်းကတော့ စာမျက်နှာတိုင်းအတွက် https သုံးတဲ့ ကွန်ယက်အခြေပြုအသုံးချနည်းလမ်းများကို ရှာဖွေပါ။

စိစစ်ရေးကို ရှောင်ရှားခြင်း

ကွန်ယက်အခြေပြု ပရောက်ဆီ (Proxies) များ၊ စိစစ်ရေးရှောင်တိမ်းတဲ့ အသုံးချကိရိယာများ သို့မဟုတ် Tor လို ကိုယ့်ရဲ့ IDကိုဖျောက်ပေးတဲ့ အမည်မဖော်တဲ့ဆော့ဖ်ဝဲများကို ဖာ်ဆိုဒ်သွားကြည့်တဲ့အခါ သို့မဟုတ် စောင့်ကြည့်ခံထားရတဲ့ အင်တာနက်ကော်နက်ရှင်များကို သုံးတဲ့အခါသုံးနိုင်တယ်။ ဒီနည်းလမ်းတွေဟာ ပိတ်ထားခံရတဲ့ ဖာ်ဆိုဒ်များ ဥပမာ - သုတေသနမလုပ်နိုင်အောင် သို့မဟုတ် Facebook လို ကွန်ယက်အခြေပြု ပလက်ဖောင်းများကို update လုပ်ခြင်းက တားဆီးနိုင်အောင်ပါ။

အွန်လိုင်းပေါ်မှာ လူသိမခံပါနှင့်

သွားကြည့်တဲ့ ဖာ်ဆိုဒ်များကို ဖုံးကွယ်လိုလျှင် Tor လို အမည်မဖော်တဲ့ ဆော့ဖ်ဝဲများက အသုံးဝင်ပါတယ်။ Tor ဟာ ISP နဲ့ အင်တာနက်ပေါ် လှုပ်ရှားမှုများကို အစိုးရအဆင့် အင်တာနက်ပေါ် စောင့်ကြည့်သူများရန်က ကင်းဝေးအောင် ကော်နက်ရှင်များကို အခြားအခမဲ့ ကူညီပေးတဲ့ ကွန်ပျူတာများအကြား ဟိုဒီပို့ပေးပြီး ကာကွယ်ပေးပါတယ်။ သို့သော်လည်း လုံခြုံမှုမရှိတဲ့ ဖာ်ဆိုဒ်များဆီ ပေါက်ကြားလို့လုံးဝမဖြစ်တဲ့ သတင်းအချက်အလက်များ ပေးပို့ခြင်းနဲ့ လက်ခံခြင်းအတွက်တော့ Tor ကို မသုံးပါနဲ့။ ဒါပေမဲ့ HTTPS သုံးထားတဲ့ ဖာ်ဆိုဒ်နဲ့ ဆက်သွယ်ထားမယ်ဆိုရင်တော့ အခမဲ့ကူညီထားတဲ့ ကွန်ပျူတာတွေက တစ်လုံးက တင်ပို့နေတဲ့ အကြောင်းအရာတွေကို စောင့်ကြည့်ပေးထားမယ်ဆိုတာမျိုးက ဖြစ်နိုင်ချေရှိပါတယ်။ Tor က လုံခြုံရေးအတွက်တော့ တော်တော်စိတ်ချရပါတယ်။ ဒါပေမဲ့ အင်တာနက်ကော်နက်ရှင်ကို နေးစေပါတယ်။

မိုဘိုင်းဖုန်းများ

ကွန်ဟာနဲ့အပှမ်း မိုဘိုင်းဖုန်းကို ကျယ်ကျယ်ပြန့်ပြန့် သုံးစွဲပါတယ်။ ဒါပေမဲ့ လူသိမခံအပ်တဲ့ သတင်းအချက်အလက်တော်တော်များများကိုလည်း သိမ်းဆည်းထားတတ်ကြတယ်။ ဒါ့အပြင် ဆက်သွယ်ရန်လိပ်စာတွေ၊ ဖုန်းခေါ်ထားတဲ့ ရာဇဝင်တွေ၊ အစီအစဉ်ဇယားတွေ၊ စာတိုများ နဲ့ အီးမေးလ်များလည်းရှိပါသေးတယ်။

အထူးသဖြင့် တယ်လီဖုန်း အချက်အလက်များကို အလွယ်သိမ်းယူနိုင်တဲ့အတွက်ကြောင့် ဖုန်းထဲမှာ အချက်အလက်သိမ်းဆည်းခြင်းကို ဂရုပြုပါ။ ဥပမာ - ပေါက်ကြားလို့လုံးဝ မဖြစ်နိုင်တဲ့ ကိစ္စများကို ကိုင်တွယ်နေရပြီဆိုရင်တော့ ဆက်သွယ်ရန်လိပ်စာများကို ဖုန်းထဲ ထားစရာ မလိုပါဘူး။ ဒါ့အပြင် ဖုန်းထဲမှာရော Sim ကဒ်ထဲမှာပါ ရှိတဲ့အချက်အလက်များကိုလည်း ဖျက်ဖို့မမေ့ပါနဲ့။ ပွဲတခုကိုစီစဉ်နေမယ်၊ ကွန်ယက်ပေါ်မှာ စည်းရုံးရေးလုပ်နေမယ်ဆိုရင် အမည်မဖော်ဝဲနေခြင်း၊ ကြိုတင်ငွေပေးချေစနစ်နဲ့ ဖယ်ရတဲ့ Sim ကဒ်များသုံးခြင်းနဲ့ လက်ကိုင်ဖုန်းအခွံများ မကြာခဏပြောင်းခြင်းတို့ လုပ်သင့်ပါတယ်။ စာတို (SMS) ပို့ခြင်းဟာ အလွယ်တကူစစ်ကြည့်လို့ ရတဲ့အတွက် စာတိုများပို့ပေးတဲ့အခါ အရေးကြီးတဲ့စကားလုံးများ သုံးခြင်းကို ရှောင်သင့်တယ်။ မိုဘိုင်းဖုန်းဖွင့်ထားသမျှ ကာလပတ်လုံး နေရာကို ခြေရာခံလို့ ရတယ်။ အရေးကြီးတဲ့ ချိန်းဆိုပွဲတွေကို တက်သူတွေ ပြန်သွားပြီးချိန်အထိ ဖုန်းများကိုပိတ်ခိုင်းပြီး ဓာတ်ခဲများပါ ဖြုတ်ထားခိုင်းသင့်ပါတယ်။ မိုဘိုင်းဖုန်းဖန်ဆင်မှုပေးသူတွေဟာ ဘယ်သူ့ဆီကို ဘယ်အချိန်မှာ ဘယ်နေရာက ဖုန်းခေါ်ဆိုတယ်ဆိုတာအားလုံးကို ကြည့်လို့ရပါတယ်။ တဖန်ရှိသူများက တောင်းဆိုလာခဲ့ရင် တယ်လီဖုန်းဖန်ဆောင်မှုပေးသူတွေက ဒီအသေးစိတ်အချက်အလက်များကို တရားဥပဒေအရ ကူးယူထားခွင့် ထုတ်ပြန်ခွင့် ရှိပါတယ်။ တခါတရံ ကာလအတိုင်းအတာတခုအထိ သိမ်းဆည်းထားပေးရတာမျိုးတွေလည်း ရှိပါတယ်။

လေ့ကျင့်ခန်း။ ။ လုံခြုံရေးအတွက် အန္တရာယ်ရှိနိုင်တာများကို လေ့လာခြင်း
အောက်ဖော်ပြပါမေးခွန်း သုံးပြီး ရှိနိုင်မယ့် လုံခြုံရေးအန္တရာယ်များကို လေ့လာကာ ဘယ်နည်းလမ်းကို အသုံးပြုကာကွယ်နိုင်မလဲ ဆုံးဖြတ်ပါ။

၁။ **အရေးကြီးတဲ့ သတင်းအချက်များကို ကိုင်တွယ်နေရပါတယ်။** ။ ကိုယ်တွယ်နေရတဲ့ သတင်းအချက်အလက်များဟာ စောင့်ကြည့်ခြင်းခံနိုင်ရလောက်အောင် အရေးကြီးခြင်း ရှိမရှိသိဖို့ အရေးကြီးပါတယ်။ အစိုးရ၊ ရဲ၊ စစ်တပ် သို့မဟုတ် သီးခြားပုဂ္ဂိုလ်တဦးရဲ့ ကိုယ်ပိုင်ကုမ္ပဏီ စသူတွေရဲ့ အဖျက်လုပ်ငန်းယူဆနိုင်လောက်တဲ့ လှုပ်ရှားမှုတခုမှာ ပါနေသလား။ ပါနေရင် လုံခြုံရေးနဲ့ ပတ်သက်ပြီး ကာကွယ်မထားရင် ကိုယ်တိုင်နဲ့ အနားကလူများအတွက် အန္တရာယ်ရှိနိုင်ပါတယ်။

၂။ **မည်သူမည်ပါဆိုတာနဲ့ အသေးစိတ်အချက်အလက်များကို လျှို့ဝှက်ရမည့်သူများနဲ့ အလုပ်လုပ်ကိုင်နေရပါတယ်။** ။ အိမ်တွင်းအကြမ်းဖက်မှု၊ အတင်းအဓမ္မခိုင်းစေခြင်း (သို့) မုဒိမ်းမှုစတာတွေနဲ့ ပတ်သက်တဲ့ အချက်အလက်များကို ထောက်ပံ့ပေးတဲ့လူဆီက လျှို့ဝှက်အချက်အလက်တွေ ရယူနေတဲ့အခါမျိုးမှာ ဒီထောက်ပံ့ပေးသူတွေအတွက် အန္တရာယ်ရှိနိုင်လို့ သေချာစွာလျှို့ဝှက်ထားသင့်ပါတယ်။

၃။ **တခါတရံ အရေးကြီးတဲ့ သတင်းများကိုင်တွယ်နေရတဲ့ လူများနဲ့ အွန်လိုင်းမှာ ဆက်သွယ်ရပါတယ်။** ။ ကိုယ်တိုင် အန္တရာယ်မရှိလောက်ပါဘူးလို့ ထင်နေသည့်တိုင် အတူလုပ်ကိုင်နေသူရဲ့ အန္တရာယ်ရှိနိုင်တဲ့ အနေအထားကြောင့် ထိုသူကိုတိုက်ခိုက်သူများရဲ့ သတင်းအချက်အလက်နောက်လိုက်ရန် ပစ်မှတ်ဖြစ်တတ်ပါတယ်။ တခြားသူများရဲ့ လျှို့ဝှက်အချက်အလက်များအတွက် အသုံးချခံဖြစ်သွားနိုင်ပါတယ်။

၄။ **ဟာ်ဆိုဒ်များပေါ် ပေါက်ကြားရန်မဖြစ်သင့်တဲ့ အချက်အလက်များကို ကြည့်နေတယ် သို့မဟုတ် တင်ပို့နေတယ်။** ။လူအခွင့်အရေး ဟာ်ဆိုဒ်တွေမှာ သတင်းအချက်အလက်ပေမျှခြင်း သို့မဟုတ် ဆန့်ကျင်နေတဲ့အဖွဲ့က လူအခွင့်အရေးခံ ပျိုးဖောက်နေတာများကို ထောက်ပြခြင်း စသည်တို့ဖြစ်ပါတယ်။ ဒီလို အန္တရာယ်များတဲ့ ဟာ်ဆိုဒ်များကိုသာ ဟင်ရောက်ကြည့်ခြင်းဟာ သတိထားမိစေတဲ့အချက်များ ဖြစ်ပါတယ်။

အင်တာနက် လုံခြုံရေးနှင့် ကာကွယ်ရန် အရင်းအမြစ်များ

လုံခြုံရေးနဲ့ပတ်သက်တဲ့အကြောင်းများ ပိုလေ့လာရန်နဲ့ လုံခြုံရေးနည်းလမ်းများ ဒေါင်းလုဒ်လုပ်ရန်

၁။ **Tactical Tech နဲ့ Front Line တို့ရဲ့ (Security in-a-box)** သေတ္တာထဲမှ လုံခြုံရေးဆိုတဲ့ ဆော့ဖ်ဝဲကတော့ လှုံ့ဆော်ရေးသမားများနဲ့ လူအခွင့်ရေးကာကွယ်သူများရဲ့ ဒစ်ဂျစ်တယ်လုံခြုံရေးနဲ့ ထိုသူတို့ရဲ့ ကိုယ်ရေးကိုယ်တာလုံခြုံရေး လိုအပ်ချက်များအတွက် ရည်ရွယ်ပါတယ်။

၂။ **ဒစ်ဂျစ်တယ်လုံခြုံရေးနဲ့ လူအခွင့်အရေးကာကွယ်သူများအတွက် သိုသိပ်စွာနေခွင့် ဆိုတဲ့ ဆော့ဖ်ဝဲကိုတော့ ဒစ်ဂျစ်တယ်ခြိမ်းခြောက်မှုများ** သိရှိထောက်ပြနိုင်တဲ့ အသုံးကျတဲ့ အချက်အလက်များနဲ့ တကွ Front Line က ထောက်ပံ့ပေးပါတယ်။

၃။ **Tactical Tech ရဲ့ (Mobile in-a-box)** သေတ္တာတွင်းက မိုဘိုင်းဆိုတဲ့ ဆော့ဖ်ဝဲမှာတော့ မိုဘိုင်းဖုန်းများနဲ့ ပတ်သက်သမျှ လုံခြုံရေးနှင့် ကိုယ်ရေးကိုယ်တာ လုံခြုံရေးအတွက် ဖြစ်ပါတယ်။ http://mobiles.tacticaltech.org/security

၄။ **Global Voices ရဲ့ Wordpress & Tor သုံးပြီး** အမည်မဖော်ပဲ ဘလော့ရေးနည်းကတော့ အမှန်တရားဘက်က ရပ်တည်ပြီး အမှန်တရားအတွက်ကာကွယ်လိုတဲ့ အခွင့်အရေးထောက်ခံရေးသမားများ ဘယ်လို အန္တရာယ်ကင်းကင်း လုပ်ကိုင်နိုင်တာကို လမ်းညွှန်ပေးပါတယ်။ http://advocacy.globalvoicesonline.org/projects/guide/

၅။ **အွန်လိုင်းပေါ်မှာ အမည်မသိစေရန်နဲ့ စိစစ်ရေးကို ရှောင်လွှဲနိုင်ရန် နည်းလမ်းများ။** Tor ဆိုတဲ့ ဆော့ဖ်ဝဲဟာ အွန်လိုင်းလှုပ်ရှားမှုများကို အမည်မဖော်ပဲ လှုပ်ရှားနိုင်ပြီး အင်တာနက် စိစစ်မှုတွေကိုလည်း ရှောင်ရှားနိုင်ပါတယ်။ ဒီဆော့ဖ်ဝဲကို ကွန်ပျူတာထဲ ဒေါင်းလုဒ်လုပ်ထားနိုင်ပြီး USB Device ကလည်း သုံးနိုင်ပါတယ်။ http://www.torproject.org/

TACTICAL TECHNOLOGY COLLECTIVE