Canada

CENTRE FOR LAW AND DEMOCRACY

MPC

စာနယ်ဇင်းသမားများအတွက် ဒစ်ဂျစ်တယ်လုံခြုံရေးလမ်းညွှန်

ဒီဇင်ဘာလ ၂၀၁၇

ims

INTERNATIONAL MEDIA SUPPORT

FOJO:MEDIA INSTITUTE
Linnæus University

စာနယ်ဇင်းသမားများအတွက် ဒစ်ဂျစ်တယ်လုံခြုံရေးလမ်းညွှန်[1]

အောက်တိုဘာလ ၂၀၁၇

၁။ နိဒါန်း

အင်တာနက် နှင့် အခြားဒစ်ဂျစ်တယ်နည်းလမ်းဖြင့် ဆက်သွယ်ရေးတို့သည် သတင်းအချက်အလက် ရယူသုံးစွဲခွင့်အား အကြီးအကျယ် မြှင့်တင်ပေးထားသောနည်းဖြင့် ထောက်ပံ့ပေးပါသည်။ ထို့အပြင် လွတ်လပ်စွာ ထုတ်ဖော်ပြောဆိုခွင့်ကို ရယူခံစားနိုင်ရန် အဓိကအကျဆုံး သယ်ဆောင်ပေးရာ နည်းတစ်ခုအဖြစ် ထမ်းဆောင်ပေးပါသည်။ အလားတူ စာနယ်ဇင်းလောကတွင် လက်တွေ့လုပ်ကိုင်ကျင်လည်မှုများအတွက် ပို၍ကျယ်ပြန့်သော အင်တာနက် နှင့် ဒစ်ဂျစ်တယ်ဆက်သွယ်ရေးတို့၏ အကျိုးကျေးဇူးသည် အလွန်တရာကြီးမားပါသည်။ အင်တာနက်သည် စာနယ်ဇင်းသမားများအတွက် သုတေသန ပြုလုပ်ရန် ရနိုင်သော အရင်းအမြစ်များကို ကြီးမားစွာ မြှင့်တင်ပေးသည်။ သတင်းပေးသူ နှင့် ထိတွေ့မှု ပြုလုပ်ကာ ဆက်သွယ်နိုင်သည့် နည်းလမ်း နှင့် အကြောင်းအရာကို ဖြန့်ဝေရန် နှင့် သူတို့၏ပရိသတ်များ နှင့် ဆွေးနွေးမှုပြုလုပ်ရန် လမ်းကြောင်းတို့ကိုလည်း ကြီးမားစွာ မြှင့်တင်ပေးပါသည်။

တစ်ချိန်တည်းတွင် စာနယ်ဇင်းသမားများသည် အွန်လိုင်းလောကအတွင်း ခြိမ်းခြောက်မှုများစွာကို ရင်ဆိုင်ခဲ့ရပြီးဖြစ်ကာ ၊ ရှေ့ဆက်၍လည်း ရင်ဆိုင်နေရမည် ဖြစ်သည်။ ဆက်သွယ်ရေးပုံစံကို ဒစ်ဂျစ်တယ်နည်းသို့ ပြောင်းလဲလိုက်ခြင်းသည် ၎င်းနှင့်အတူ အလွန်ကြီးမားစွာ မြင့်တက်လာသည့် အစွမ်းသတ္တိ နှင့် စောင့်ကြည့်ထောက်လှမ်းခြင်းနည်းလမ်း (နိုင်ငံအစိုးရ များထံမှရော အစိုးရ မဟုတ်သည့် အုပ်စုများထံကပါ) တို့ဖြင့် စာနယ်ဇင်းသမားများအတွက် ခြိမ်းခြောက်မှုအသစ်များ

[1] Portia Karegeya, ဥပဒေရေးရာအရာရှိ ၊ ဥပဒေ နှင့် ဒီမိုကရေဒီရေးရာ စင်တာ က မူကြမ်းရေးဆွဲသည်။ ဤအစီရင်ခံစာကို အများပြည်သူဆိုင်ရာ မူပိုင်ခွင့် ကင်းလွတ်မှုသတ်မှတ်ချက်-စီးပွားရေးဖြင့်မဆိုင်သော-ဝေမျှနိုင်သော မူကွဲ ၃.၀ နေရာဒေသအလိုက် ပြုပြင်မထားသော လိုင်စင် (Creative Commons Attribution-NonCommercial-ShareAlike 3.0 Unported Licence) ရယူထားသည်။ သင်သည် ဥပဒေ နှင့် ဒီမိုကရေစီ ရေးရာ စင်တာမှ ရယူထားကြောင်း အသိအမှတ်ပြုဖော်ပြပြီး စီးပွားရေးအတွက် အသုံးမပြုဘဲ ဤထုတ်ဝေမှုမှ ဆင့်ပွားဖန်တီးသမျှ ဤလိုင်စင် စည်းကမ်း သတ်မှတ်ချက်ဖြင့်ထပ်တူ ဖြန့်ဖြူးမည်ဆိုပါက ဤအစီရင်ခံစာကို လွတ်လပ်စွာ မိတ္တူကူးယူ၊ ဖြန့်ဖြူး၊ ပြသပြီး ဆင့်ပွား ဆောင်ရွက်နိုင်သည်။ ဤလိုင်စင်၏မိတ္တူကို ကြည့်ရှုရန် ဤဝက်ဘ်ဆိုက်တွင် ကြည့်ရှုနိုင်သည်။ http://creativecommons.org/licenses/by-nc-sa/3.0/.

ဆောင်ယူလာခဲ့ပါသည်။ ထိုသို့သော ခြိမ်းခြောက်မှုများတွင် အခြားနည်းများအပြင် တည်နေရာ ခြေရာခံလိုက်ခြင်းသော်လည်းကောင်း၊ အချက်အလက်နှိုက်ထုတ်ရယူခြင်း(Data mining) ဖြစ်စေ၊ ဆက်သွယ်ရေးကြားဖြတ်ဖမ်းယူခြင်းဖြစ်စေ၊ နှစ်ခုစလုံးဖြစ်စေ ပြုလုပ်ခြင်းသော်လည်းကောင်း ပါဝင်နိုင်သည်။ ဤကဲ့သို့သော အနေအထားတွင် စာနယ်ဇင်းသမားဘက်က လျှို့ဝှက်ပေးထားရမည့် သတင်းပေးသူ မည်သူမည်ဝါဖြစ်ကြောင်း အထောက်အထားကို အကာအကွယ်ပေးခြင်း အပိုင်းအရ အထူးတလည် စိန်ခေါ်မှုဖြစ်လာကြောင်း တွေ့ရပါသည်။

နောက်ထပ် အန္တရာယ်မှာ အွန်လိုင်းအပေါ်မှ အနှောင့်အယှက်ပေးမှု အထူးသဖြင့် လူမှုမီဒီယာ ပလက်ဖောင်းပေါ်မှ အနှောင့်အယှက်ပေးမှု အဆင့် ကြီးထွားလာနေခြင်း ဖြစ်သည်။ အွန်လိုင်း အပေါ်မှ အနှောင့်အယှက်ပေးခြင်း အတွက် တိကျသော အဓိပ္ပါယ်ဖွင့်ဆိုချက် မရှိပါ။ သို့သော် Pew Research Center က ၎င်းသည် အောက်ပါ အခြေခံသဘောတရား ခြောက်ခုမှ တစ်ခုခု ပါဝင်သည်ဟု ထူးခြားသည့် လက္ခဏာများကို ဖော်ထုတ်ပေးထားသည်။ ၎င်းတို့မှာ ထိခိုက်စော်ကားသည့် အမည်ဖြင့် အခေါ်ခံရခြင်း၊ အရှက်ခွဲရန် တမင်သက်သက် အားစိုက်ဆောင်ရွက်ခြင်း ၊ ရုပ်ပိုင်းအရ ခြိမ်းခြောက်ခံရခြင်း ၊ နောက်ယောက်ခံ အလိုက်ခံရခြင်း ၊ အဆက်မပြတ် ရှည်ကြာစွာ အနှောင့်အယှက်အပေးခံရခြင်း နှင့် လိင်ပိုင်းဆိုင်ရာအရ အနှောင့်အယှက်အပေးခံရခြင်းတို့ဖြစ်သည်။ [2]

အွန်လိုင်းအပေါ်မှ အနှောင့်အယှက်ပေးမှုသည် အဓိကအားဖြင့် ကျား/မရေးရာကိစ္စ နှင့် သက်ဆိုင်လျက်ရှိပြီး အများအားဖြင့် အမျိုးသမီးများသည် အွန်လိုင်းအပေါ်မှ အနှောင့်အယှက်ပေးမှုကို ပိုမိုမြင့်မားသည့် အဆင့်ဖြင့် ရင်ဆိုင်ရလေ့ရှိသည်။ အွန်လိုင်းအပေါ်မှ အနှောင့်အယှက်ပေးမှု အပေါ် ၂၀၁၄ ခုနှစ် Pew Research Centre ၏ စစ်တမ်းတစ်ခုက အမျိုးသမီးငယ်များသည် အခြားသူများထက်စာလျှင် ပိုမိုပြင်းထန်သော အနှောင့်အယှက်ပေးမှုပုံစံကို ပို၍ကြုံတွေ့ရနိုင်ဖွယ်ရာရှိပြီး အထူးသဖြင့် ရုပ်ပိုင်းဆိုင်ရာ ခြိမ်းခြောက်မှု နှင့် ကာလရှည် အဆက်မပြတ် အနှောင့်အယှက်ပေးမှု အပြင် အွန်လိုင်းနောက်ယောက်ခံလိုက်ခြင်း နှင့် လိင်ပိုင်းအရ အနှောင့်အယှက်ပေးခြင်းကို ပိုမို၍ ခံစားရနိုင်ကြောင်း တွေ့ရှိခဲ့ရသည်။ [3] ၂၀၁၇ ခုနှစ်တွင် ဤစစ်တမ်းကို နောက်ထပ်တစ်ကြိမ် ထပ်မံ၍ ပြုလုပ်ခဲ့ရာ အလားတူရလဒ်ပဲ ပေါ်ထွက်ခဲ့သည်။ အမျိုးသားများသည် အမျိုးသမီးများထက်စာလျှင် အွန်လိုင်းအပေါ်တွင် အနှောင့်အယှက်ပေးခံရမှု အတော်အတန် ပိုများနိုင်သော်လည်း အမျိုးသမီးများသည် အွန်လိုင်းအပေါ်တွင် လိင်ပိုင်းဆိုင်ရာ အနှောင့်အယှက်ပေးမှု၏ ပစ်မှတ်ထားခံရသူများ ပို၍ ဖြစ်နိုင်ဖွယ်ရာရှိသည်။[4]

စာနယ်ဇင်းသမားများအပေါ် အလေးပေးသော လေ့လာမှုများကလည်း ခြိမ်းခြောက်မှုများကို အမျိုးသမီးများ နှင့် အမျိုးသားများအကြား အကြမ်းဖျဉ်းတူညီသော နှုန်းထားဖြင့် တွေ့ကြုံရကြောင်း

---

[2] Maeve Duncan, *Online Harassment,* Pew Reaserch Center, 22 October 2014, p. 5. Available at: http://www.pewinternet.org/2014/10/22/part-1-experiencing-online-harassment/#demographics-of-online-harassment.

[3] *၎င်း*

[4] Maeve Duncan, *Online Harassment,* Pew Reaserch Center, 11 July 2017. Available at: http://www.pewresearch.org/fact-tank/2017/07/11/key-takeaways-online-harassment/.

တွေ့ရှိခဲ့ရသည်။ ခြွင်းချက်အနေဖြင့် လိင်ပိုင်းဆိုင်ရာ အနှောင့်အယှက်ပေးမှု နှင့် ပတ်သက်လာသည့်အခါ အမျိုးသမီးများက မကြာခဏပိုပြီး ခံစားရပါသည်။ [5] ဥရောပအတွင်း လုံခြုံရေး နှင့် ပူးပေါင်းဆောင်ရွက်ရေး (Security and Co-operation in Europe – OSCE) အတွက် အဖွဲ့အစည်း၏ မီဒီယာလွတ်လပ်ခွင့် ကိုယ်စားလှယ်က ထိုအမြင်ကို ထင်ဟပ်ပြီး " အမျိုးသမီးစာနယ်ဇင်းသမားများ၊ ဘလော့ဂ်ဂါများ နှင့် အခြားမီဒီယာလုပ်ငန်း လုပ်ကိုင်သူများသည် အင်တာနက် အပေါ်တွင် ကျား/မ ရေးရာ နှင့် သက်ဆိုင်သော ခြိမ်းခြောက်မှုများ ၊ အနှောင့်အယှက်ပေးမှု နှင့် အကြပ်ကိုင်မှုတို့ကို အချိုးအစားမမျှတစွာ တစ်ဖက်သတ် တွေ့ကြုံ ခံစား နေရသည် " ဟု တင်ပြထားသည်။ [6] ကင်ညာနိုင်ငံတွင် ဤကဲ့သို့သောပုံစံဖြင့် အပြင်းထန်ဆုံးဖြစ်ရပ်များတွင် အမျိုးသမီးစာနယ်ဇင်းသမားများသည် အချိန်ကာလတာတစ်ခုအထိ စာနယ်ဇင်းသမားအဖြစ် အလုပ်လုပ်ခြင်း မှ ရပ်ဆိုင်းခြင်း သို့မဟုတ် အင်တာနက်မှ လုံးဝစွန့်ခွာသွားခြင်းပင် ဖြစ်စေခဲ့ကြောင်း တွေ့ရှိခဲ့ရသည်။ [7]

ဤပြဿနာများကို ကိုင်တွယ်ဖြေရှင်းရန် စာနယ်ဇင်းသမားများသည် ကျားမ မရွေး သူတို့ကိုယ်သူတို့ ကာကွယ်ရန် လိုအပ်သည့် အဆင့်များ လုပ်ဆောင်ထားသင့်သည်။ ဒစ်ဂျစ်တယ် တိုက်ခိုက်မှု ကိုယ်တိုင် နှင့် ၎င်းကို ဆောင်ရွက်သည့်သူများ နှစ်မျိုးစလုံးကို အဆင့်မြင့် နည်းပညာ ကျွမ်းကျင်မှု များမပါဘဲ ခွဲခြားဖော်ထုတ်ရန် ခက်ခဲနိုင်သည်ကို ထည့်တွက်လျှင် ထိုသို့လုပ်ဆောင်ရန် အထူးတလည် လိုအပ်ပါသည်။ [8] နောက်ဆုံးတွင် အမှန်တကယ် ရည်ရွယ်တိုက်ခိုက်သူများထံမှ အကြွင်းမဲ့ အကာအကွယ်ပေးရန် အာမခံထားသည့် နည်းလမ်းမရှိသော်လည်း ကောင်းမွန်သည့် ဒစ်ဂျစ်တယ် လုံခြုံရေး အလေ့အထများက ကြီးမားသည့် ကွာခြားချက် ဖြစ်သွားစေနိုင်ပါသည်။ အမျိုးသမီးစာနယ်ဇင်းသမားများသည် သူတို့ကိုယ်သူတို့ အချို့သော အွန်လိုင်း အနှောင့်အယှက်ပေးမှုပုံစံမှ ကာကွယ်ရန် နောက်ထပ်အဆင့်များ လုပ်ဆောင်ထားသင့်သည်။ သို့သော် ဤလမ်းညွှန်စာတမ်းသည် စာနယ်ဇင်းသမားအား သူတို့ ကိုယ်ပိုင် ဒစ်ဂျစ်တယ်လုံခြုံရေးအပြင် သူတို့၏ လုပ်ဖော်ကိုင်ဖက်များ နှင့် သတင်းပေးများကိုကာကွယ်ရန် လိုအပ်သည့်နည်းလမ်းများအား ရယူသုံးစွဲနိုင်ပြီး နားလည်ရန်လွယ်ကူသော ပုံစံ ဖြင့် ထောက်ပံ့ပေးရန် ရည်ရွယ်ပါသည်။

---

5 Elana Newman, *et al.*, "Online abuse of women journalists: Towards an Evidence-based Approach to Prevention and Intervention" in OSCE, Representative on Freedom of the Media, *New Challenges to Freedom of Expression: Countering Online Abuse of Female Journalists,* 2016, p. 49. Available at: http://www.osce.org/fom/220411?download=true.
6 Recommendations following the Expert Meeting New Challenges to Freedom of Expression: Countering Online Abuse of Female Journalists, 17 September 2015, in OSCE, Representative on Freedom of the Media, *New Challenges to Freedom of Expression: Countering Online Abuse of Female Journalists,* 2016, p. 5. Available at: http://www.osce.org/fom/220411?download=true.
7 ARTICLE 19 and AMWIK, *Women Journalist's Digital Security* [sic], May 2016, p. 4. Available at: https://www.article19.org/data/files/medialibrary/38757/Women-Journalist's-Digital-Security-Kenya-2016.pdf.
8 Jennifer R. Henrichsen, *et al.*, *Building Digital Safety for Journalism: A survey of selected issues*, UNESCO Series on Internet Freedom, 2015, p. 14. Available at: http://unesdoc.unesco.org/images/0023/002323/232358e.pdf.

၂။ ခြိမ်းခြောက်မှုပုံစံငယ်ဖော်ထုတ်ယူခြင်း နှင့် အန္တရာယ် အကဲဖြတ်ဆန်းစစ်ခြင်း

ဒစ်ဂျစ်တယ်လုံခြုံရေးကို အာမခံနိုင်ရန် ပထမဆုံးအဆင့်တွင် စာနယ်ဇင်းသမားများ နှင့် သတင်းအဖွဲ့အစည်းများအတွက် ဖြစ်နိုင်ခြေရှိသော လုံခြုံရေးခြိမ်းခြောက်မှုများအတွက် ခြိမ်းခြောက်မှုပုံစံငယ်ထုတ်ယူခြင်း -threat modelling နှင့် အန္တရာယ်အကဲဖြတ်ဆန်းစစ်ခြင်း - risk assessment ကိစ္စကိုဆောင်ရွက်ရန် အရေးကြီးပါသည်။ ရည်မှန်းချက်မှာ ခြိမ်းခြောက်မှုကို ပို၍ခန့်မှန်းမိခြင်း သို့မဟုတ် လျှော့၍ခန့်မှန်းမိခြင်းတို့မှ ရှောင်ရှားရန်အတွက် ဖြစ်သင့်ပါသည်။ ၎င်းအစား စောင့်ကြည့်ထောက်လှမ်းခြင်း ၊ အနှောင့်အယှက်ပေးခြင်း နှင့် တစ်စုံတစ်ဦး၏ ဒစ်ဂျစ်တယ်ဆိုင်ရာလှုပ်ရှားမှုများအပေါ် ဖြစ်နိုင်ဖွယ်ရှိသော ဖမ်းယူသိမ်းဆည်းမှုတို့၏ အန္တရာယ်ကိုသင့်တော်စွာခွဲခြား ဖော်ထုတ်ရန် နှင့် ၎င်းတို့ကိုကာကွယ်ရေး အတွက် သင့်တော်သော ဆောင်ရွက်ဖွယ်ရာ အဆင့်များ လုပ်ဆောင်ရန် ဖြစ်သင့်ပါသည်။ [9]

The Electronic Frontier Foundation (EFF) က ခြိမ်းခြောက်မှု ပုံစံငယ်တစ်ခု ဖန်တီးရာတွင် လူများသည် အောက်ပါ မေးခွန်း ငါးခုကို မေးမြန်းသင့်ကြောင်း အကြံပြုထားပါသည်။ [10]

၁. မိမိသည် မည်သည့်အရာကို ကာကွယ်လိုသနည်း။

သင့်တွင်ရှိသည့် တန်ဖိုးရှိပြီး အကာအကွယ်ပေးရန် လိုအပ်သော သတင်းအချက်အလက် နှင့် အရင်းအမြစ်များကို စဉ်းစားသုံးသပ်ပါ။ ၎င်းတို့အထဲတွင် သင်၏ တည်နေရာ ၊ အဆက်အသွယ် စာရင်းများ ၊ ကိရိယာများ ၊ ဖိုင်များ နှင့် စာရွက်စာတမ်းများ ပါဝင်သည်။ ထို့အပြင် ထိုသတင်းအချက်အလက်ကို သိုလှောင်ထားသည့် နေရာ နှင့် နည်းလမ်း ၊ ၎င်းကို ရယူသုံးစွဲခွင့်ရှိသည့်သူများ နှင့် သတင်းအချက်အလက် ရယူသုံးစွဲမှုအား ကန့်သတ်နိုင်သည့် နည်းလမ်းများကို စာရင်းပြုစုပြီး ထည့်သွင်းစဉ်းစားသင့်သည်။

၂. မိမိသည် ၎င်းကို မည်သူ့ထံမှ ကာကွယ်လိုသနည်း။

မည်သည့် လူပုဂ္ဂိုလ် သို့မဟုတ် အဖွဲ့အစည်းများက သင် သို့မဟုတ် သင်၏ သတင်းအချက်အလက်အား ပစ်မှတ်ထားနိုင်ခြေ ရှိသည်ကို စေ့စေ့စပ်စပ် စဉ်းစားပါ။ ဤစာရင်းထဲတွင် တစ်သီးပုဂ္ဂလများ ၊ ကော်ပိုရေးရှင်းများ သို့မဟုတ် နိုင်ငံအစိုးရအဆင့်အထိ ပါဝင်နိုင်သည်။

---

[9] Della Kilroy, The Storyful Podcast: Digital Security – How Journalists and Activists Can Be Protected Online, Storyful, 31 January 2017. Available at: https://storyful.com/blog/2017/01/31/the-storyful-podcast-digital-security-how-journalists-and-activists-can-be-protected-online/.

[10] EFF, Surveillance Self-defense: Assessing Your Risks. Available at: https://ssd.eff.org/en/module/assessing-your-risks.

၃. မိမိ၏ကာကွယ်မှုသာကျရှုံးခဲ့မည်ဆိုလျှင်အကျိုးဆက်သည် မည်မျှဆိုးဝါးနိုင်သနည်း။

ဒစ်ဂျစ်တယ်နည်းအရ တိုက်ခိုက်သူများ၏ ရည်မှန်းချက်များမှာ မည်သည့်အရာများ ဖြစ်နိုင်သည်ကို စဉ်းစားပါ။ ဥပမာ သင်သည် ဗီဒီယိုဖိုင် တစ်ခုမှ ရရှိသောအကြောင်းအရာ အတွက် သတင်းတစ်ခု ပို့ပေးနေသည်ဆိုလျှင် တစ်စုံတစ်ယောက်က ထို ဗီဒီယိုကို သင်၏ ကိရိယာထဲမှ ဖျက်ပစ်လိုခြင်း ရှိလာနိုင်သည်။ ထိုလုပ်ရပ်သည် သင်၏ သတင်းအောင်မြင်မှု အတွက် အနည်း နှင့် အများဆိုသလို အရေးကြီးနိုင်သည်။

၄. မိမိက ၎င်းကို အကာအကွယ်ပေးရန် လိုအပ်မှု မည်မျှအထိ ဖြစ်နိုင်ခြေ ရှိသနည်း။

တိုက်ခိုက်မှုတစ်ခု အမှန်တကယ်ဖြစ်လာနိုင်ခြေ သို့မဟုတ် အန္တရာယ်ကိုစဉ်းစားသုံးသပ်ပါ။ ဥပမာ ဖုန်းကုမ္ပဏီတစ်ခုသည် ပုံမှန်အားဖြင့် သင်၏ ဖုန်းမှတ်တမ်းများကို ရယူသုံးစွဲခွင့် ရှိသော်လည်း သူတို့က ထိုမှတ်တမ်းများကို အသုံးပြုပြီး သင့်အား ထိခိုက်အောင် ပြုလုပ်ရန် ဖြစ်နိုင်ခြေမှာ အလွန် နည်းပါသည်။ အခြားတနည်း ဆိုရလျှင် မည်သည့် ခြိမ်းခြောက်မှုများသည် အမှန်တကယ်ဖြစ်ပေါ်လာရန် ဖြစ်နိုင်ခြေ ပိုများပြီး မည်သည့် ခြိမ်းခြောက်မှုများက ဖြစ်တန်စွမ်း နည်းပါးသည်ကို စဉ်းစားသုံးသပ်ပါ။

၅. ဖြစ်လာနိုင်သော အကျိုးဆက်များကို ကာကွယ်ရန် ကြိုးစားရာတွင် မိမိသည် မည်မျှအထိ ဒုက္ခခံလိုစိတ် ရှိပါသနည်း။

ဒစ်ဂျစ်တယ်တိုက်ခိုက်မှုများကို ကာကွယ်ရန် သင့်တွင်ရှိသည့် ရွေးချယ်စရာများကို စဉ်းစားသုံးသပ်ပါ။ ထို့နောက် ထိုရွေးချယ်စရာကို အကောင်အထည် ဖော်ရင်းဖြင့် သင့်အနေဖြင့် ရင်ဆိုင်ရဖွယ်ရာရှိသော နည်းပညာဆိုင်ရာ၊ ဘဏ္ဍာရေးဆိုင်ရာ နှင့် လူမှုရေးဆိုင်ရာ အကန့်အသတ်များကို စဉ်းစားသုံးသပ်ပါ။ အချို့သော ခြိမ်းခြောက်မှုများသည် ကာကွယ်ရန် ခက်ခဲလွန်းနေနိုင်သည်။

ဤနေရာတွင် ထည့်သွင်းစဉ်းစားစရာမှာ ဖြစ်နိုင်ဖွယ်ရှိသော ရန်ဘက်များ ၊ တစ်ဦးတစ်ယောက်ချင်း ရပ်တည်သော hacker များ ၊ ပုဂ္ဂလိကပိုင်ကုမ္ပဏီများ နှင့် အစိုးရလုပ်ငန်း အကောင်အထည်ဖော်သူများသည် သင်၏ အချက်အလက်ကို ပေါက်ကြားစေရန် စိတ်ဝင်စားမှု နှင့် စွမ်းဆောင်ရည်အဆင့်မှာ အမျိုးမျိုးကွဲပြားနေနိုင်သည်။ ပုံမှန်အားဖြင့် အစိုးရသည် အားလုံးအထဲတွင် အကြီးမားဆုံး စွမ်းဆောင်ရည် ရှိသည်။

ခြိမ်းခြောက်မှုပုံစံငယ် ဖော်ထုတ်ယူခြင်းသည် တစ်ကြိမ်သာလုပ်ရမည့် လုပ်ငန်းစဉ် မဟုတ်ဘဲ စာနယ်ဇင်းသမား အလုပ်လုပ်ကိုင်ရာ နောက်ခံအဆက်အစပ် နှင့် အခြေအနေ ပြောင်းလဲသည့်အခါ တဖန်ပြန်၍ လုပ်ဆောင်သင့်ပါသည်။[11]

၃။ *Passwords*

ကျွန်တော်တို့၏ ဒစ်ဂျစ်တယ် account များ နှင့် ဝန်ဆောင်မှု များစွာသည် ပုဂ္ဂိုလ်ရေးဆိုင်ရာ အကြောင်းအရာ နှင့် အချက်အလက်များ ပါဝင်ပြီး ၎င်းတို့သည် ပေါက်ကြားရန် အားနည်းချက် ရှိပါသည်။ Password များသည် ထိုဝန်ဆောင်မှုများကို အပြင်လူများ ရယူသုံးစွဲခြင်းမှ ကာကွယ်ရန် သော့ပိတ်ထားခြင်းအတွက် အရေးကြီးသော နည်းလမ်းတစ်ခု ဖြစ်သည်။

a) အားကောင်းသော Passwords

အားကောင်းသော password များ ဖန်တီးသတ်မှတ်ရန်မှ အလွန်အရေးကြီးပါသည်။ ဤနေရာတွင် ကံအကြောင်းမလှသည့် စိန်ခေါ်မှုမှာ password များသည် လူတစ်ဦးအတွက် မှတ်မိရန် ခက်ခဲနေချိန်တွင် ၎င်းတို့အား ကွန်ပျူတာတစ်လုံးက အလွယ်တကူ တွက်ချက် ဖော်ထုတ်နိုင်ခြင်း ဖြစ်သည်။ လက်တွေ့ အသုံးတည့်သည့် အကြံပြုချက်သုံးခုမှာ အောက်ပါ အတိုင်းဖြစ်သည်။

၁. ကျပန်း စာလုံးများ ၊ ကိန်းဂဏန်းများ နှင့် အထူးအက္ခရာများ ရောစပ်ပြီး အသုံးပြုပါ။
၂. ရှည်လေ ၊ ကောင်းလေ ဖြစ်သည်။ အက္ခရာ ၁၂ လုံး သို့မဟုတ် ထို့ထက်ကျော်လျှင် ပိုကောင်းသည်။
၃. တူညီသော password တစ်ခုတည်းကို sites/services များစွာ အတွက် အသုံးပြုခြင်းမှ ရှောင်ကြဉ်ပါ။

Password များ ဖန်တီးသည့်အခါ သုံးခု သို့မဟုတ် ထို့ထက်ပိုသော ကျပန်း စကားလုံးများ တွဲစပ်ပြီး ပြုလုပ်ထားသည့် *passphrase* အသုံးပြုမှုကို အကြံပေးထောက်ခံထားသည်။ ထို စကားလုံးတွဲများသည် မှတ်ဉာဏ်ထဲမှ ပြန်လည်ဖော်ယူရန် ပို၍ လွယ်ကူပြီး ၎င်းတို့၏ ရှည်လျားမှုကြောင့် hack လုပ် ချိုးဖောက်ရန် ခက်ခဲသည်။ (ဉပမာ cowplantfridgeshoes)

သင်၏ passphrase တွင် ကျပန်းဖြစ်မှုအဆင့်ကို မြှင့်တင်ရန် Diceware နည်းစနစ်ဟု ခေါ်သော နည်းလမ်းကို သုံးနိုင်သည်။ ၎င်းသည် Diceware Word List.[12] ဟုခေါ်သော စာရင်းတစ်ခုမှ

[11] *၎င်း*

စကားလုံးများကို ကျပန်းရွေးချယ်ရန် အံစာတုံးကို အသုံးပြုပြီး passphrase များ ရွေးကောက်ယူသော နည်းလမ်းဖြစ်သည်။ စာရင်းထဲမှ စကားလုံး တစ်ခုချင်းစီသည် ၁ မှ ၆ အထိပါသော ကိန်းဂဏန်းများ နှင့် ဖွဲ့စည်းထားသည့် ကိန်းလုံးရေ ၅ လုံးပါ နံပါတ် တစ်ခုနှင့် သက်ဆိုင်သည်။ Passphrase ကို ရွေးချယ်ခြင်းအတွက် ဤနည်းလမ်းကို အသုံးပြုမည်ဆိုလျှင် တစ်ခု သို့မဟုတ် တစ်ခုထက်ပိုသော အံစာတုံး လိုအပ်သည်။ (ဘုတ်ပြားသုံး ကစားနည်းတွင် ပါသော အံစာတုံး (သို့) အရုပ်ဆိုင် (သို့) ဝါသနာရှင်များအတွက်ဖွင့်သော စတိုးဆိုင်တို့တွင် သီးခြားရောင်းသော အံစာတုံး ကိုလည်း သုံးနိုင် ပါသည်။) အံစာတုံးတစ်ခုကို ငါးကြိမ်ခေါက်ခြင်း သို့မဟုတ် အံစာတုံး ငါးတုံးကို တစ်ကြိမ် တည်းခေါက်ခြင်း သို့မဟုတ် သင့်စိတ်ကြိုက် အခြား ပေါင်းစပ်မှု အမျိုးမျိုးတို့ဖြင့် အညွှန်းကိန်းရှာရမည်။ ဂဏန်းငါးလုံးပါသည့် ကိန်းဂဏန်းရသည် နှင့် တပြိုင်နက် Diceware စကားလုံး စာရင်းတွင်ကြည့်ပြီး သက်ဆိုင်ရာ စကားလုံးကို သင်၏ passphrase တစ်ပိုင်း အဖြစ် ရွေးယူရမည်။ ထိုလုပ်ငန်းစဉ်ကို သင်၏ passphrase အတွင်း သင်ထည့်သွင်း လိုသလောက် စကားလုံးရေ များများရအောင် ထပ်ခါတလဲလဲ လုပ်ဆောင်ပါ။ ရှည်လျားလေ ပိုကောင်းလေဖြစ်သည်။ [13]

b) Password Managers

Password managers သည် လူအများစု အတွက် platform များစွာတွင် သုံးစွဲရန် လိုအပ်သော password ပေါင်းများစွာကို စီမံခန့်ခွဲခွင့်ပြုသည့် အွန်လိုင်း tool တစ်ခုဖြစ်သည်။ Password managers သည် သင့်ဘက်မှနေ၍ master password တစ်ခု ဖန်တီးရန် လိုအပ်သည်။ (သင့်အနေဖြင့်မှတ်မိနေရန် လိုအပ်သည့်တစ်ခုတည်းသောအရာ။ ထို့ကြောင့် ၎င်းသည် အားကောင်း သင့်သည်။)ထို ပင်မ password သည်သင့်အား password manager ထဲသို့ ဝင်ခွင့်ပြုပြီး ၎င်းသည် သင်၏အခြား password များအားလုံး ပါရှိသည့်စာဝှက်နည်းဖြင့်သိမ်းဆည်းထားသော ဘဏ္ဍာတိုက် encrypted vault ပုံစံ သဖွယ် ဖြစ်နေသည်။ ယနေ့ခေတ်တွင် password manager များသည် ကိရိယာ များစွာတွင် တပြိုင်တည်း ချိန်ညှိယူရန် syncing လုပ်ခြင်း ၊ သင့်ကိုယ်စား သင်၏ account ထဲ ဝင်ပေးသည့် ကိရိယာတစ်ခုတည်း အတွင်းတွင် ရှိနေခြင်း သို့မဟုတ် သင့်အနေဖြင့် နေရာ များစွာတွင် password တစ်ခုတည်း အသုံးမပြုရန် သေချာစေခြင်း ကဲ့သို့ အမျိုးမျိုးသော ရွေးချယ် စရာများကို ထောက်ပံ့ပေးသည်။ [14]

---

[12] Dice-Indexed Passphrase Word List. Available at: http://world.std.com/~reinhold/dicewarewordlist.pdf

[13] www.diceware.com တွင်ကြည့်ပါ။

[14] Allan Henry, *The Five Best Password Managers*, Lifehacker, 22 August 2017. Available at: https://lifehacker.com/5529133/five-best-password-managers.

ထိရောက်သော password managers အချို့တွင် အောက်ပါတို့ပါဝင်သည်။ -

- LastPass
- KeePass
- Dashlane
- Roboform 8
- 1Password

c) Two-Factor Authentication[15]

သင်၏ အွန်လိုင်း account များအတွက် two-factor authentication ကို သုံးစွဲနိုင်ရန် ဖွင့်ပေးထားခြင်းသည် အွန်လိုင်းလုံခြုံရေးကို မြှင့်တင်ရန် အရိုးရှင်းဆုံး နှင့် အကောင်းဆုံး နည်းလမ်း တစ်ခု ဖြစ်သည်။ Two-factor authentication တွင် password တစ်ခုအပြင် သင့်အား account ထဲ ဝင်ခွင့်မပြုမီ နောက်ထပ် 'အကြောင်းအရာ' တစ်ခု သို့မဟုတ် အချက်အလက် တစ်ခု သွင်းပေးရန် လိုအပ်သည်။ ဤအချက်အလက်သည် ပုံမှန်အားဖြင့် သင့်ထံ စာသားသတင်းတို ၊ အီးမေးလ် သို့မဟုတ် သတ်မှတ်ထားသည့် app တစ်ခုမှ တစ်ဆင့် ပေးပို့သည့် အထူးသီးသန့် code တစ်ခု ပုံစံ ရှိပါသည်။ အထက်တွင်ဖော်ပြခဲ့သော LastPass ကဲ့သို့ password manager များသည် ၎င်းတို့၏ လုံခြုံရေးရွေးချယ်စရာ နည်းလမ်းတစ်ပိုင်း အဖြစ် two-factor authentication ကို ထည့်သွင်းပေးထားသည်။ Google, Yahoo, Facebook, Twitter နှင့် Dropbox အပါအဝင် အဓိက အွန်လိုင်း ဝန်ဆောင်မှုအားလုံးသည် two-factor authentication ကိုပေးကမ်းထားပါသည်။

Authy သည် စိတ်ဝင်စားစရာကောင်းသော two-factor authentication application တစ်ခု ဖြစ်သည်။

> Code တစ်ခုကို စနစ်ချိုးဖောက်အချက်အလက်ရယူထိန်းချုပ်မှု -hacking သို့မဟုတ် စောင့်ကြည့်ခြင်းတို့မှ ခုခံနိုင်စွမ်းအားနည်းနိုင်သည့် စာသားသတင်းတို သို့မဟုတ် အီးမေးလ် တို့မှတစ်ဆင့် ပို့ဆောင်မည့်အစား Authy application ကို သင်၏ ကိရိယာ ထဲသို့ download ချယူရပြီး two-factor authentication code များကို အလိုအလျောက် ထုတ်ပေးပါသည်။ အင်တာနက် သို့မဟုတ် မိုဘိုင်းလ်ဖုန်း cell ဝန်ဆောင်မှု မပါရှိဘဲ offline ပုံစံ ဖြစ်သဖြင့် စောင့်ကြည့်ခြင်း သို့မဟုတ် hacking တို့ရန်မှ နှိုင်းယှဉ်ချက်အရ ဘေးကင်းပါသည်။ ထို့အပြင် သင်၏ Authy-registered two-factor account များကို encrypted cloud တစ်ခုထဲတွင် အရန်သိုလှောင်ထားသဖြင့် Authy server များ hack အလုပ် ခံရသည့်တိုင် သင်၏အချက်အလက်အား အကာအကွယ်ပေးထားပြီးသား ဖြစ်နေပါလိမ့်မည်။

[15] Google, 2-Step Verification. Available at: https://www.google.com/landing/2step/.

၄။ Email Encryption

အီးမေးလ်သည် လူမှုမီဒီယာ နှင့် မိုဘိုင်းလ် application ပုံစံအမျိုးမျိုးတို့နှင့်အတူ ဒစ်ဂျစ်တယ်နည်းအရ ဆက်သွယ်ခြင်း၏ အသုံးအများဆုံး နည်းလမ်းတစ်ခုဖြစ်သည်။ အီးမေးလ် ဆက်သွယ်ရေးများကို ကာကွယ်ရန် အဆင့်မြင့် ရှုပ်ထွေးပြီး လုံခြုံရေး မြင့်မားသော နည်းလမ်းတစ်ခုမှာ ၄င်းတို့ကို စာဝှက်နည်းဖြင့် encrypt ပြုလုပ်ရန်ဖြစ်သည်။ Encryption ကို အီးမေးလ် နှင့် အခြားဒစ်ဂျစ်တယ်ဖိုင်များ နှင့် ဆက်သွယ်ရေးများ အပေါ်တွင် အသုံးချသည့်အခါ ပါဝင်သည့် အကြောင်းအရာ အချက်အလက်ကို ဒစ်ဂျစ်တယ် နည်းဖြင့် ဝှက်စာ ပုံစံပြောင်းလိုက်ပါသည်။ ထို့ကြောင့် အများအားဖြင့် 'secret key' ဟု ခေါ်လေ့ရှိသည့် ထိုဝှက်စာကို ပြန်ဖော်ပေးသော ဝှက်စာဖော် သော့ချက်မရှိသူအတွက် အဓိပ္ပါယ်ဖော်မရဘဲ ဖြစ်နေပါလိမ့်မည်။

Pretty Good Privacy (PGP) သည် အီးမေးလ် နှင့် ဖိုင်များကို encrypting လုပ်ရန် နည်းပညာတစ်ခုဖြစ်ပြီး hacker များအနေဖြင့် ၄င်းတို့ကို ဝင်ရောက်သုံးစွဲခွင့် ရရှိရန် ပို၍ ခက်ခဲစေသည်။ ၄င်းက သင်၏ အီးမေးလ်များသည် ရည်စူးသည့်သူသာ ဖတ်ရှုနိုင်စွမ်း ရှိရန် သေချာစေပြီး လက်ခံရရှိသူသည် ထိုအီးမေးလ်များကို ဝှက်စာပုံစံမှ ပြန်ဖော်ရန် password တစ်ခု အသုံးပြုဖို့ လိုအပ်သည်။ PGP သည် သင့်အနေဖြင့် သင်၏ အီးမေးလ်ကို ဒစ်ဂျစ်တယ်နည်းဖြင့် လက်မှတ်ရေးထိုးခွင့်လည်း ပြုပြီး မည်သူက ပို့ဆောင်သည် ဆိုသည်ကို သက်သေအထောက်အထား ထောက်ပံ့ပေးသည်။

PGP ကိုတပ်ဆင်အသုံးပြုခြင်းသည် ရှုပ်ထွေးပွေလီသော လုပ်ငန်းစဉ် တစ်ခုဖြစ်သည်။ EFF က Windows နှင့် OS X နှစ်မျိုးစလုံးအတွက် PGP တပ်ဆင်ထည့်သွင်းရန် နည်းလမ်း အတွက် အသေးစိတ်ညွှန်ကြားချက်များ ထောက်ပံ့ပေးထားသည်။

၅။ သာမန် Hacking and Phishing တို့ရန်မှ အကာအကွယ်ယူခြင်း

ပုဂ္ဂိုလ်ရေးအချက်အလက်များ ရယူရန် hacker များ သုံးစွဲသည့် အသုံးအများဆုံး နည်းလမ်းတစ်ခုမှာ phishing ဖြစ်သည်။ Phishing နည်းဖြင့် တိုက်ခိုက်ခြင်းသည် အမြဲအားဖြင့် ဘဏ်တစ်ခုကဲ့သို့ တရားဝင် ဝက်ဘ်ဆိုက်မှ ပို့ဆောင်ပုံရသည့် အီးမေးလ် တစ်စောင် အသွင်ယူလေ့ရှိသည်။ ၄င်းတွင် link တစ်ခုပါပြီး ထိုနောက်ကို လိုက်လံကြည့်ရှုပါက password တစ်ခုကဲ့သို့ ပုဂ္ဂိုလ်ရေးအကြောင်းအရာကို ထည့်သွင်းရန် တောင်းခံမည်ဖြစ်သည်။ အီးမေးလ်သည် မှတ်တမ်းဖိုင်တစ်ခုကို download ချရန် သို့မဟုတ် ဆော့ဖ်ဝဲ တစ်ခုကို တပ်ဆင်ထည့်သွင်းရန်လည်း တောင်းခံနိုင်သည်။ ထိုကဲ့သို့ ပြုလုပ်ခြင်းသည် malware ဟု ခေါ်ကြသည့် အနှောင့်အယှက်ပေးသော မလိုတမာ ဆော့ဖ်ဝဲ ကို သင်၏ ကိရိယာအတွင်း တပ်ဆင်ထည့်သွင်းခံရသည့် အဖြစ်သို့ ရောက်ရှိသွားစေမည်ဖြစ်သည်။ ထိုနောက် တိုက်ခိုက်သူများသည် သင်၏ ကိရိယာကို အဝေးမှ ရယူသုံးစွဲရန် သို့မဟုတ် သင်၏ သတင်းအချက်အလက်များ ခိုးယူရန် သို့မဟုတ် သင့်ကို စောင့်ကြည့်ထောက်လှမ်းရန် ထို malware ကို အသုံးပြုနိုင်ပါသည်။

Phishing တိုက်ခိုက်မှုများမှ သင့်ကိုယ်သင် ကာကွယ်ရန် အကြံပြုချက်အချို့မှာ အောက်ပါ အတိုင်း ဖြစ်သည်။ -

- သင့်အနေဖြင့် လက်ခံရရှိရန် မျှော်လင့်မထားသည့် အီးမေးလ်မှတစ်ဆင့် သင့်ဆီ ပို့ဆောင်လာသည့် link များကို ကလစ် မနှိပ်ပါနှင့်။ အကယ်၍ သံသယရှိပါက အီးမေးလ်ကို ပို့ဆောင်သူက အမှန်တကယ်ပေးပို့သလားဆိုသည်ကို မှန်ကန်ကြောင်း စစ်ဆေးရန် အခြားနည်းလမ်းကို အသုံးပြုပါ။ ဥပမာ ဘဏ် သို့မဟုတ် သင့်ဆီ အီးမေးလ် ပို့သည်ဟု ယူဆရသည့် ပုဂ္ဂိုလ်ထံ ဖုန်းဆက်ပါ။
- ဆော့ဖ်ဝဲ update များကို ဖြစ်နိုင်သမျှ အမြန်ဆုံး တပ်ဆင်ထည့်သွင်းပါ Hacker များသည် သူတို့၏ phishing အစီအမံများ ဆောင်ရွက်ရန် ဆော့ဖ်ဝဲ bug အပေါ် အမှီပြုသည်။ ဆော့ဖ်ဝဲကို နောက်ဆုံး အခြေအနေအထိ update လုပ်ထားခြင်းသည် ဤအန္တရာယ်ကို လျော့ပါးစေသည်။
- အီးမေးလ်တစ်စောင်သည် မည်မျှအထိ ပညာရှင်ဆန် သပ်ရပ်သည့် ပုံပေါက်ပါစေ ပုဂ္ဂိုလ်ရေး အချက်အလက်များကို တောင်းခံသည့် အီးမေးလ်ကို ယုံကြည်စိတ်ချခြင်း မပြုပါနှင့်။ ၎င်းတို့သည်ယုံကြည်စိတ်ချရသည့် အရင်းအမြစ်ကလာကြောင်း သိမထား လျှင် ဖြစ်ပါသည်။
- အလိုအလျောက်ဖြည့်ပေးသည့် auto fill လုပ်ဆောင်ချက်ပါသော password manager များကို အသုံးပြုပါ သင်သည် password manager တစ်ခုကို တပ်ဆင်ထည့်သွင်းပြီး ၎င်းအတွင်းတွင် သင်၏ password အမျိုးမျိုးကို သိမ်းဆည်းထားသည့်အခါ သင်က အခြား တနည်းတဖုံ သတ်မှတ်ထားခြင်းမရှိလျှင် ၎င်းသည် အများအားဖြင့်သင့်အတွက် သိမ်းဆည်းထားသည့် account များအတွင်း password တစ်ခုကို အလိုအလျောက် ဖြည့်သွင်းပေးသည်။ သင်သည် link တစ်ခုနောက်မှလိုက်ပြီး page တစ်ခုသို့ ရောက်လာသည့် အခါတွင် သင်၏ password manager က ၎င်းပုံစံအတွင်း အလိုအလျောက် မဖြည့်သွင်းလျှင် သင်ရောက်ရှိနေသည့် ဆိုက်နေရာကို နှစ်ခါပြန်စစ်ဆေးရန် လိုအပ်ကြောင်း သဲလွန်စပင် ဖြစ်သည်။ ထို့အပြင် သင်လက်ခံရရှိသည့် link များ၏ URL တို့ကို အသေအချာ ဂရုတစိုက် စေ့ငုကြည့်ပါ။၎င်းတို့တွင် စာလုံးပေါင်းအမှားများ သို့မဟုတ် ထူးဆန်းသည့် top-level domain များ ပါရှိနေနိုင်သည်။ (top-level domain သည် '.com' ကဲ့သို့ ဝက်ဘ်လိပ်စာတစ်ခု၏ နောက်ဆုံးအပိုင်းကို ရည်ညွှန်းသည်။) ဥပမာ "www.transferwise.com"သည် "www.*tras*ferwise.com" သို့မဟုတ် "www. transfer wise.*cam*" အဖြစ်ပေါ်နေနိုင်သည်။ "https://*wwwtransferwise*.com " အတွင်း မသိမသာ သိမ်မွေ့လွန်းပြီးအလွယ်တကူ သတိလက်လွတ် ဖြစ်သွားနိုင်သည့် 'www' နောက်မှ အစက်တစ်စက် မပါရှိမှုကိုလည်း သတိပြုပါ။ ထို့အပြင် gmail.com မှ 'L' သည် အမြင်အာရုံလှည့်စားရန် '*gmaiI*' မှာကဲ့သို့ 'i' အကြီးဖြင့် အစားထိုးထားနိုင်သည်ကိုလည်း သတိပြုပါ။

- သံသယရှိသည့် မည်သည့် စာရွက်စာတမ်း document မဆို Google Drive အတွင်းတွင် ဖွင့်ပါ။ ဤသို့ပြုလုပ်ခြင်းက document ကို ရုပ်ပုံတစ်ခု သို့မဟုတ် HTML အဖြစ် ပြောင်းလဲပေးပြီး သင်၏ ကိရိယာအပေါ် malware တင်ဆင်ထည့်သွင်းခြင်းမှ ကာကွယ်ပေးသည်။
- Facebook, Google (သို့) Twitter တို့မှတစ်ဆင့် ဝက်ဘ်ဆိုက်များအတွင်း ဝင်ရောက်ခြင်းမှာ ရှောင်ရှားပါ။ အွန်လိုင်းဝန်ဆောင်မှုများစွာသည် သင်၏ လူမှုမီဒီယာ account များမှတစ်ဆင့် ဝန်ဆောင်မှုအတွင်း log in ဝင်ရောက်ရန် ရွေးစရာကို ကမ်းလှမ်းထားသည်။ တရားမဝင်သော ဝက်ဘ်ဆိုက်များသည် ပုဂ္ဂိုလ်ရေး အချက်အလက်များ နှင့် password များ ရယူစုဆောင်းရန် ထိုနည်းလမ်းကို အသုံးပြုနိုင်သည်။ ထိုသို့ ပြုလုပ်မည့်အစား ဝက်ဘ်ဆိုက်အတွက် သီးသန့် ရည်ရွယ်ထားသော account သစ်တစ်ခုဖန်တီးပါ။

ယေဘုယျစည်းမျဉ်းအရ မလိုအပ်ဘဲ နှင့် ပုဂ္ဂိုလ်ရေး အချက်အလက်များ ပေးကမ်းခြင်းကို ရှောင်ကြဉ်ပါ။ ပေးရမည်ဆိုလျှင် ပုဂ္ဂိုလ်ရေး နှင့် မဆိုင်သော သတင်းအချက်အလက် (အချက်အလက်မှား)ကိုပေးပါ။ ကြိမ်ရေ အနည်းငယ်သာ အသုံးပြုလိုသော ဝက်ဘ်ဆိုက်များတွင် register လုပ်ရန် စွန့်ပစ်နိုင်သော တစ်ခါသုံး အီးမေးလ်လိပ်စာတစ်ခုကို အသုံးပြုပါ။ www.sharklasers.com ဝက်ဘ်ဆိုက်သည် စွန့်ပစ်နိုင်သော အီးမေးလ်လိပ်စာများ ထုတ်လုပ်ပေးရန် ဝန်ဆောင်မှုတစ်ခု ထောက်ပံ့ ပေးသည်။

နောက်ဆုံးတွင် သင်သည် သင်အသုံးပြုသည့် လူမှုမီဒီယာ ဝန်ဆောင်မှုများ၏ ကိုယ်ပိုင်လွတ်လပ်ခွင့် သတ်မှတ်ချက်များ - privacy settings များ နှင့် လုံခြုံရေးစွမ်းဆောင်ရည်များနှင့် ရင်းနှီးကျွမ်းဝင်နေကြောင်းသေချာအောင်လုပ်ရမည်။ အောက်တွင် စာနယ်ဇင်းသမားများ အသုံးအများဆုံး platform အချို့၏ ကိုယ်ပိုင်လွတ်လပ်ခွင့် လမ်းညွှန်ချက်များအတွက် link များ ဖော်ပြပေးထားသည်။

- Facebook
- Twitter
- Linkedin

၆။ လုံခြုံပြီး သုံးစွဲသူ မည်သူမည်ဝါဖြစ်ကြောင်း မသိနိုင်သည့် အင်တာနက် ရှာဖွေကြည့်ရှုသွားလာခြင်း

သင်၏ အင်တာနက် ရှာဖွေကြည့်ရှုမှုသည် လုံခြုံမှုမရှိပါက ကိုယ်ပိုင်လွတ်လပ်ခွင့် ရှိမည်မဟုတ်ပါ။ အသုံးပြုသူ၏ ရွေးချယ်မှုအကြိုက်များကို ခြေရာခံမှတ်သားရန် သင်၏ ကွန်ပျူတာပေါ်တွင် ဝက်ဘ်ဆိုက်များက အလိုအလျောက် သိမ်းဆည်းထားသည့် အချက်အလက် အပိုင်းအစလေးများဟု အရှင်းဆုံး ဖော်ပြနိုင်သည့် Cookies များသည် ဝက်ဘ် အပေါ်တွင် ရှာဖွေကြည့်ရှု

သွားလာခြင်း ၏ အခြေခံကျသော အစိတ်အပိုင်း တစ်ခုဖြစ်သည်။ ယခုအခါ cookies များသည် သင်၏ သုံးစွဲမှု ဆိုင်ရာ တွေ့ကြုံခံစားမှု အကြောင်း အချက် အလက်ကို သိမ်းဆည်းရန်သာမက သင်၏ တစ်ဦးချင်း အွန်လိုင်းအပြုအမူ အကြောင်း အချက်အလက်ကို ခြေရာကောက်ရန် အတွက်လည်း အသုံးပြုသည်ကို နေရာတကာ တွေ့လာရပါသည်။ Cookies များက သိမ်းဆည်း ထားသည့် သတင်း အချက်များကို ဈေးကွက်မြှင့်တင်ရေးကုမ္ပဏီများက လွန်စွာတန်ဖိုး ထားပြီး ၎င်းတို့က သူတို့၏ ကြော်ငြာ များကို ပို၍ကောင်းစွာ ပစ်မှတ်ထားနိုင်ရန် ပုဂ္ဂိုလ်အလိုက် ကောက်ကြောင်းများ တည်ဆောက်ရန် အသုံးပြုကြသည်။၎င်းအချက်အလက်ကို ကာလရှည်ကြာစွာ စုဆောင်းယူပြီး မကြာခဏဆိုသလို သင်၏သိရှိမှု သို့မဟုတ် သဘောတူခွင့်ပြုမှုမရှိဘဲ ဖြန့်ဝေလေ့ ရှိကြသည်။ဆိုလိုသည်မှာ ၎င်းသည် သင်၏အကြောင်း အချက်အလက်ကို မကောင်းသော ရည်ရွယ်ချက်အတွက် အသုံးပြုလိုသည့် လုပ်ငန်းဆောင်ရွက်သူများ လက်ထဲကျရောက်သွားနိုင် သလား ဆိုသည် သိရှိရန် နည်းလမ်းမရှိဘဲ ဖြစ်နေပါသည်။

အများသုံး Wi-Fi သည် လုံခြုံမှု အထူးတလည် ကင်းမဲ့သည့်နေရာဖြစ်သည်။ ကွန်ရက်တစ်ခုကို password ဖြင့် ကာကွယ်ပေးထားသော်လည်း ကွန်ရက်ကို အသုံးပြုနေသော အခြားသူများသည် ဝက်ဘ်အပေါ် သင်၏ ရှာဖွေကြည့်ရှုသွားလာခြင်းကို စောင့်ကြည့်ထောက်လှမ်းနိုင်စွမ်း ရှိနိုင်သည်။ ၎င်းနည်းအားဖြင့် သင့်အကြောင်း ပုဂ္ဂိုလ်ရေးအချက်အလက်ကို ကြီးမားသည့် ပမာဏ ဖြင့် စုဆောင်းရန် ဖြစ်နိုင်ခြေရှိသည်။ အင်တာနက် ရှာဖွေကြည့်ရှုသွားလာခြင်း browsing ပြုလုပ်စဉ်တွင် လုံခြုံရေးကိုမြှင့်တင်ရန် နည်းလမ်းများစွာ ရှိပါသည်။ Chrome, Safari, Internet Explorer နှင့် Firefox ဟူသည့် လူကြိုက်အများဆုံး browser အများစုထဲတွင် Firefox သည် သုံးစွဲသူ၏ ရပိုင်ခွင့်များ အကာအကွယ်ပေးခြင်းအတွက် အကျော်ကြားဆုံးသော ဂုဏ်သတင်းရှိသည်။ အခြား browser များကို ထိန်းချုပ်ထားသည့် ကုမ္ပဏီများသည်သုံးစွဲသူ၏ အပြုအမူများအား ခြေရာကောက် ခဲ့ကြောင်း ကြားသိခဲ့ရပြီးဖြစ်သည်။ ရလဒ်အဖြစ် သင်၏ default browser အဖြစ် Firefox ကို သုံးစွဲရန် အကြံပြုထားပါသည်။

a) Browser Extensions

Browser extension များသည် သင်၏ အင်တာနက် browser သို့ ပေါင်းထည့်နိုင်သည့် အခမဲ့ ရသော ဖြည့်စွက်စွမ်းရည်များဖြစ်ပြီး သင်၏ အင်တာနက်အပေါ် ရှာဖွေကြည့်ရှုသွားလာမှုများအား hacker များ ၊ အစိုးရစောင့်ကြည့်မှု နှင့် ကော်ပိုရိတ် ကြော်ငြာပစ်မှတ်ထားခြင်းများမှ ကာကွယ်ပေး သည်။ ကာကွယ်မှု အဆင့်မြှင့်တင်ရန် browser များတွင် သင်ပေါင်းထည့်နိုင်သော extension အတော်များများ ရှိပါသည်။ -

- Privacy Badger: ကြော်ငြာရှင်များ နှင့် အခြား တတိယအဖွဲ့ ခြေရာခံလိုက်သူများ က သင်၏ အင်တာနက်အပေါ်ရှာဖွေကြည့်ရှုသွားလာခြင်း အမူအကျင့်များအား လျှို့ဝှက်စွာ ခြေရာကောက်ခြင်းကို ဟန့်တားရန် EFF က ၎င်း browser add-on ကို ဖန်တီးခဲ့သည်။ သင့်ကို ခြေရာခံလိုက်နေသည့် ကြော်ငြာရှင်များကို ထောက်လှမ်းသိရှိသည့်အခါ အကြောင်း

အရာများ သင်၏ browser အပေါ် ခေါ်တင်ရန် သူတို့၏ စွမ်းရည်ကို အလို အလျောက် ပိတ်ပင်တားဆီးပေးသည်။ ၎င်းကို Chrome, Firefox နှင့် Opera browser များတွင် တပ်ဆင်ရန် ရရှိနိုင်သည်။

- HTTPS Everywhere: EFF ကပဲဖန်တီးထားခြင်းဖြစ်သည့် ဤ extension သည် ဖြစ်နိုင်သည့်အခါတိုင်း သင်၏ ရှာဖွေကြည့်ရှုသွားလာမှု - browsing ကို အလိုအလျောက် encrypt လုပ်ပေးသည်။ ရလဒ်အဖြစ် phishing ပုံစံတိုက်ခိုက်မှုများမှ ကြီးမားစွာ အကာအကွယ်ပေးမှုကိုလည်း ပေးကမ်းပါသည်။ Privacy Badger ကဲ့သို့ ၎င်းကို Chrome, Firefox နှင့် Opera browser များတွင် တပ်ဆင်ရန် ပေါင်းထည့်နိုင်သည်။

- uBlock Origin: ၎င်းသည် သင် အင်တာနက်အပေါ် ရှာဖွေကြည့်ရှုသွားလာနေစဉ် ကြော်ငြာများကို ပိတ်ပင်တားဆီးပေးသော ad blocker extension တစ်ခုဖြစ်ပြီး ကြော်ငြာများသည် malware , viruses နှင့် မလိုလားအပ်သော ခြေရာခံလိုက်ခြင်းတို့၏ ကြီးမားသော အရင်းအမြစ် ဖြစ်ကြောင်းကို ထည့်တွက်ထားသည်။ ၎င်းကို Chrome နှင့် Firefox တွင် တပ်ဆင်ထည့်သွင်းနိုင်သည်။

- Disconnet.me: ဤ extension သည် သင်၏ ဝက်ဘ်ပိုင်းဆိုင်ရာ လှုပ်ရှားမှုများနောက် ခြေရာခံလိုက်သူများအား လိုက်လံကြည့်ရှုခြင်းမှ ပိတ်ပင်တားဆီးပြီး ပို၍မြန်ဆန်သော ရှာဖွေကြည့်ရှုသွားလာမှုကို ခွင့်ပြုသည်။ ၎င်းကို Chrome နှင့် Firefox နှစ်မျိုးစလုံး အတွက် ရရှိနိုင်သည်။

b) Tor Browser[16]

တစ်စုံတစ်ဦးသည် အထက်ပါ tool များအားလုံး သုံးနေသည့် အခါမှာပင် အဆင့်မြင့် hacker များ ၊ အစိုးရ၏လုပ်ငန်း အကောင်အထည်ဖော်ပေးနေသူများ နှင့် အင်တာနက်ဝန်ဆောင်မှုပေးသူများသည် သင့် ကွန်ပျူတာ၏ ပုဂ္ဂလိက Internet Protocol (IP) လိပ်စာ နှင့် သင့် ကွန်ပျူတာမှ အသွားအပြန်ပို့ဆောင်ပေးနေသော သတင်းအချက်အလက်များကို အခြေခံပြီး သင်၏ တည်နေရာကို ရှာဖွေနိုင်စွမ်း ရှိနေဆဲပဲ ဖြစ်ပါသည်။ ဤထောက်လှမ်းမှုမှနေ၍ မည်သည့် extension မှ ကာကွယ်ပေးနိုင်ခြင်း မရှိပါ။ ထို့ကြောင့် သင်သည် အင်တာနက်အပေါ် ရှာဖွေကြည့်ရှုသွားလာရင်း မည်သူမည်ဝါမှန်း လုံးဝ မသိစေလိုလျှင် Tor Browser ကို သုံးစွဲခြင်းအား စဉ်းစားသင့်သည်။

Tor browser သည် Tor network မှတစ်ဆင့် လည်ပတ်လုပ်ဆောင်ပြီး ကမ္ဘာတစ်ဝန်း နေရာအနှံ့ ခုန်ပေါက်ရွှေ့ပြောင်းနေရင်း နှင့် မတူကွဲပြားသော encryption အလွှာအထပ် အဆင့်ဆင့် တို့မှ

16 EFF, How HTTPS and Tor Work Together to Protect Your Anonymity and Privacy. Available at: https://www.eff.org/pages/tor-and-https.

တစ်ဆင့် သင်၏ ဝက်ဘ်ပိုင်းဆိုင်ရာ ဆက်သွယ်မှု မူလအစနေရာကို ခြေရာမခံနိုင်ရန် သေချာစေသည်။ Tor browser သည် အစိုးရ နှင့် သဘောထားဆန့်ကျင် ကွဲလွဲသူများ သို့မဟုတ် မတရားမှု ဖော်ထုတ်အသိပေးသူများ - whistleblower ကဲ့သို့ မည်သူမည်ဝါ ဖြစ်ကြောင်း လျှို့ဝှက်ထားရန် အရေးအကြီးဆုံး ဖြစ်သည့် သတင်းပေးများ နှင့် စာနယ်ဇင်းသမားများ အကြား လုံခြုံသော ဆက်သွယ်ရေးအတွက် အထူးတလည် အသုံးဝင်ပါသည်။ Tor browser သည် မည်သူမည်ဝါမှန်း မသိဘဲ အင်တာနက်အပေါ် ရှာဖွေသွားလာကြည့်ရှုခြင်းကို ထောက်ပံ့ပေးရုံမက သုံးစွဲသူများအတွက် Tor network မှတစ်ဆင့်သာ ရယူကြည့်ရှုနိုင်မည့် ဝက်ဘ်ဆိုက်များ ထူထောင်ခြင်း နှင့် သုံးစွဲခြင်းကိုလည်း ဖြစ်စေနိုင်သည်။ သို့သော် ၎င်းသည် မည်သူမည်ဝါမှန်း မသိအောင် ဖုံးကွယ်ပေးသည့်နည်းများ တစ်ဆင့်ခံ သုံးစွဲနေရသဖြင့် Tor ဖြင့် ရှာဖွေကြည့်ရှုသွားလာခြင်း သည် ပုံမှန် browser များထက် နှေးကွေးနိုင်ပါသည်။

အရေးကြီးသည့် မှတ်သားစရာခြွင်းချက်မှာ Tor က သင်၏ လှုပ်ရှားမှုများကို မည်သူမည်ဝါမှန်း မသိအောင် ဖုံးကွယ်ပေးထားချိန်တွင် သင်၏ ဆက်သွယ်မှုများကိုတော့ ကိုယ်ပိုင်သီးသန့် ဖြစ်အောင် ပြုလုပ်မပေးပါ။ သင်၏ Facebook စာမျက်နှာမှ တစ်ဆင့် စာစုများ ရေးတင်ခြင်း သို့မဟုတ် သင်၏ ကိုယ်ပိုင် အီးမေးလ် account မှ အီးမေးလ်ပို့ခြင်း တို့ကဲ့သို့ သင့်အား ခွဲခြားဖော်ထုတ်နိုင်သော အင်တာနက် လှုပ်ရှားမှုများတွင် ပါဝင်လျှင် သင့်ကို အကာအကွယ်ပေးနိုင်မည် မဟုတ်ပါ။

c) Virtual Private Network (VPN)

ပုံမှန်စံ အင်တာနက် browser များကို အသုံးပြုပြီး မည်သူမည်ဝါမှန်း မသိအောင် ထိန်းသိမ်းထားနိုင်ရန် အကောင်းဆုံးနည်းမှာ သင်၏ ဝက်ဘ်အပေါ်သွားလာမှု ကို encrypt လုပ် စာဝှက်ပေးပြီး ကြားဖြတ်ရယူခြင်းမှ ကာကွယ်တားဆီးပေးသည့် virtual private network (VPN) တစ်ခုကို အသုံးပြုရန် ဖြစ်သည်။ သင်က VPN တစ်ခုကို အသုံးပြုသည့်အခါ သင်၏ ဝက်ဘ်ပိုင်းဆိုင်ရာ တောင်းခံမှုသည် VPN server တစ်ခုကို ဖြတ်သွားရပြီး ၎င်းက သင်၏ အချက်အလက်ကို ပို၍ ကျယ်ပြန့်သော အင်တာနက်သို့ မရောက်ရှိမီ encrypt လုပ်ပေးပါသည်။ ထို့ကြောင့် သင်က ဝက်ဘ်ဆိုက်တစ်ခုသို့ ဝင်ရောက်ကြည့်ရှုသည့်အခါ သင်၏ တောင်းခံမှုသည် VPN server က လာသည့်ပုံ ပေါ်မည်ဖြစ်ပြီး ၎င်းသည် ကမ္ဘာအနှံ့ မည်သည့်နေရာတွင်မဆို တည်ရှိနေနိုင်ကာ သင်၏ အမှန်တကယ်တည်နေရာမှ လာမည့်ပုံပေါ်မည်မဟုတ်ချေ။ VPN တစ်ခုကို အသုံးပြုခြင်းသည် အများနှင့်ဆိုင်သော ကွန်ရက်ကို အသုံးပြုသည့်အခါ သင်၏ အချက်အလက်ကို encrypt လုပ်ခြင်း နှင့် သင်၏ ပုဂ္ဂိုလ်ရေး အကြောင်းအရာကို အကာအကွယ်ပေးခြင်း အပြင် အချို့သော ဝက်ဘ်ဆိုက်များအား တားမြစ်ထားသည့် network တစ်ခုမှတစ်ဆင့် ဆက်သွယ်သည့်အခါ အင်တာနက် ဆင်ဆာဖြတ်တောက်မှုကို ရှောင်ကြဉ်ရန်လည်း ကူညီပေးပါသည်။

နည်းပညာပိုင်းအရကြည့်လျှင် နားလည်တတ်ကျွမ်းသူ တစ်ဦးသည် OpenVPN ကဲ့သို့ open-source ဆော့ဖ်ဝဲကို အသုံးပြုပြီး သူတို့ကိုယ်ပိုင် VPN server များ ဆင်ယူနိုင်သည်။ သို့မဟုတ် သူတို့၏ browser များတွင် ပေါင်းထည့်နိုင်သော အခမဲ့ VPN add-ons များကို အသုံးပြုနိုင်သည်။ [17] များစွာသောသူများသည် VPN provider လုပ်ငန်းတစ်ခုတွင် လစဉ်ကြေးအဖြစ် အခကြေးငွေ ပေးချေခြင်းဖြင့်လည်း သုံးစွဲကြပြီး ထိုကဲ့သို့သော လုပ်ငန်းများတွင် ရွေးစရာများစွာရှိပါသည်။

VPN များသည် အများနှင့်ဆိုင်သော networkကို အသုံးပြုနေစဉ်တွင် စောင့်ကြည့်ထောက်လှမ်းခြင်းများမှ ကြီးမားသော အကာအကွယ်ကိုပေးသော်လည်း သင်၏ အချက်အလက်ကို VPN ကိုယ်တိုင်မှ ရယူခြင်းကို ကာကွယ်မပေးပါ။ VPN provider သည် သင်၏ လည်ပတ်သွားလာမှုများကို မြင်နိုင်စွမ်းရှိပြီး VPN provider အနေဖြင့် သင်၏ ပုဂ္ဂိုလ်ရေးအချက်အလက်ကို စုဆောင်းရယူခြင်းမှ ဟန့်တားရန် မည်သည့်နည်းမျှမရှိပါ။ ထို့ကြောင့် သင်၏ VPN ကို အသေအချာ ရွေးချယ်ရန် အရေးကြီးပါသည်။ Provider တည်ရှိသည့်နေရာကို ဂရုပြုခြင်း နှင့် ၎င်းတို့ လိုက်နာရသည့် ဥပဒေများ အကြောင်း နှင့် ၎င်းတို့၏ ကိုယ်ပိုင်လွတ်လပ်ခွင့် - privacy မူဝါဒများ အကြောင်း သိရှိအောင်ရှာဖွေခြင်းတို့ အပါအဝင် ဖြစ်သည်။ ဤနည်းအားဖြင့် အစိုးရမှ တောင်းခံမှု ပြုလုပ် လာသည့်အခါ မည်သည့် အကြောင်းအရာများသည် အစိုးရ၏ လုပ်ငန်းအကောင်အထည်ဖော် သူများထံ လွှဲပြောင်းရောက်ရှိနိုင်ဖွယ်ရာ ရှိသနည်း ဆိုသည်ကို နားလည်လာစေမည် ဖြစ်သည်။ Provider လုပ်ငန်းတစ်ခုသည် ဝန်ဆောင်မှုကို သင်အသုံးပြုနေသည့်အချိန်တွင် သင်၏ IP address ကိုလည်း ဖော်ထုတ်ရယူနိုင်စွမ်း ရှိသည်။ သင်၏ IP address ပေါက်ကြားမှုမှ ရှောင်ကြဉ်လိုလျှင် သင်၏ VPN သို့ ဆက်သွယ်ရန် Tor browser ကို အသုံးပြုနိုင်ပါသည်။ [18]

အကြံပြုထောက်ခံလိုသည့် VPN provider များမှာ အောက်ပါအတိုင်းဖြစ်သည်။ -

- AirVPN
- Feral Hosting
- CyberghostVPN

VPN တစ်ခု ထူထောင်ရန် သင်၏ ကွန်ပျူတာအပေါ်တွင် VPN client ဟုခေါ်သော အရာကို တပ်ဆင်ထည့်သွင်းရန် လိုအပ်ပြီး ၎င်းက သင်၏ VPN provider နှင့် ဆက်သွယ်ပေးသည်။ တပ်ဆင်ပြီးသည်နှင့်တပြိုင်နက် သင်၏ client ကို ကလစ်နှိပ်လိုက်ရုံဖြင့် သင်၏ အင်တာနက်အပိုင်း လှုပ်ရှားဆောင်ရွက်မှုမှန်သမျှသည် သင်၏ VPN server မှတစ်ဆင့် အလိုအလျောက် လမ်းကြောင်းရှာ သွားလာမည် ဖြစ်သည်။ VPN provider များနည်းတူ အချို့သော VPN client များအတွက် အခကြေးငွေပေးရန် လိုအပ်သော်လည်း များစွာသော client များကို အခမဲ့ရပြီး ယုံကြည်စိတ်ချမှု

[17] Preston Gralla, *5 great free VPNs for Chrome, Firefox, mobile, and beyond*, IT World, 4 August 2014. Available at: https://www.itworld.com/article/2696891/security/5-great-free-vpns-for-chrome--firefox--mobile--and-beyond.html.
[18] EFF, Surveillance-Self Defense: Choosing the VPN that's Right for You. Available at: https://ssd.eff.org/en/module/choosing-vpn-thats-right-you.

ရှိစွာ သုံးစွဲရအောင် အလုပ်လုပ်ပါသည်။ VPN provider AirVPN သည် သူ့ကိုယ်ပိုင် အခမဲ့ client နှင့် အတူလာပါသည်။ အခြား အကြံပြုထောက်ခံထားသည့် client များတွင် အောက်ပါတို့ ပါဝင်သည်။ -

- Viscosity
- Tunnelblick (free for Mac)
- OpenVPN (free for Windows)

d) Tails

Tails operating system ကိုအသုံးပြုခြင်းသည် အဆိုးစွန်အပြင်းထန်ဆုံးသော အမည်လျှို့ဝှက်မှုဆိုင်ရာ ရွေးချယ်စရာ ဖြစ်သည်။ အကြောင်းမှာ ၎င်းသည် web browser သက်သက်ဆိုသည်ထက် ပိုလွန်သောကြောင့် ဖြစ်သည်။ Tails သည် ကိုယ်ပိုင်လွတ်လပ်ခွင့် နှင့် လုံခြုံရေးကို အလေးပေးထားသည့် Linux-based operating system ဖြစ်ပြီး မည်သည့် ကွန်ပျူတာအပေါ်တွင် မဆို အချိန်မရွေး တပ်ဆင်ထည့်သွင်းနိုင်သည်။ Tails ကို အသုံးပြုခြင်းသည် စောင့်ကြည့်ထောက်လှမ်းခံရခြင်းမှ ရှောင်ရှားရန် နှင့် သူတို့၏ တည်နေရာ နှင့် အချက်အလက်ကို ပေါက်ကြားမှု မရှိစေဘဲ အင်တာနက်ကို ရယူသုံးစွဲရန် လှုပ်ရှားတက်ကြွသူများ နှင့် စာနယ်ဇင်းသမားများအတွက် အကူအညီရပါသည်။ Tails ကို USB သို့မဟုတ် DVD ထဲတွင် တပ်ဆင်ထည့်သွင်းထားနိုင်ပြီး Linux,Windows သို့မဟုတ် Apple မည်သည့် ကွန်ပျူတာတွင်မဆို အသုံးပြုနိုင်သည်။

သယ်ဆောင်ရွှေ့ပြောင်းနိုင်မှုအပြင် Tails ကို အသုံးပြုရခြင်း၏ ကြီးမားသော အကျိုးကျေးဇူးမှာ ၎င်းကို မှတ်ဉာဏ်ကွယ်အောင်ပြုလုပ်ထားသဖြင့် အသုံးပြုမှုများအကြား မည်သည့်အချက်အလက်မှ သိုလှောင်မထားသလို ခွဲခြားဖော်ထုတ်နိုင်သည့် မည်သည့် အကြောင်းအရာကိုမှလည်း ချန်ထားခဲ့ခြင်းမရှိပါ။ ထို့အပြင် အင်တာနက်ဆိုင်ရာ လှုပ်ရှားဆောင်ရွက်မှု အားလုံးသည် Tor network မှ လမ်းကြောင်းရှာပြီး HTTPS Everywhere ကိုလည်း ကြိုတင်တပ်ဆင်ထည့်သွင်းထားပြီး ဖြစ်ကာ စာဝှက်နည်းဖြင့်ပြောင်းထားသည့် အီးမေးလ်ပို့ဆောင်ခြင်းကို ဖြည့်ဆည်းထောက်ပံ့ရန် PGP email client တစ်ခုကိုလည်း ထည့်သွင်းပေးထားသည်။

လုံခြုံရေး ကိရိယာများ နှင့် ဆော့ဖ်ဝဲများ အားလုံးနည်းတူ Tails ကို အသုံးပြုသည့်အခါ သင်သည် နောက်ဆုံး version ကို သုံးစွဲနေခြင်းဖြစ်ကြောင်း သေချာစေရမည်ဖြစ်သည်။ Tails က ပိုကောင်းသော လုံခြုံရေးကို ထောက်ပံ့ပေးသော်လည်း လုံးလုံးလျားလျား လုံခြုံသောကင်းမှု မရှိပါ။

ဥပမာ Tails သည် သင်၏ မှတ်တမ်းမှတ်ရာများ ကို အလိုအလျောက် encrypt လုပ်မပေးသလို သင်၏ ကွန်ပျူတာသည် ထိခိုက်ခံရပြီးဖြစ်လျှင် သင့်ကို အကာအကွယ်ပေးနိုင်မည်မဟုတ်ပါ။ [19]

၇။ ကိရိယာပျောက်ဆုံးမှု (သို့) သိမ်းဆည်းခံရမှု

သင်၏ ကိရိယာ ပျောက်ဆုံးခြင်း ၊ အခိုးခံရခြင်း သို့မဟုတ် ယာယီအသိမ်းခံရခြင်း ဖြစ်ပွားသည့်အခါ သင်၏ အချက်အလက်များ ရယူကြည့်ရှုခြင်း သို့မဟုတ် ပေါက်ကြားထိခိုက်စေခြင်း တို့မှ ကာကွယ်ရန် ကြိုတင်ကာကွယ်မှု အဆင့်များ လုပ်ဆောင်ထားသင့်သည်။ သင်၏ အွန်လိုင်း account နှင့် ဝန်ဆောင်မှုအားလုံး လုံခြုံရေးအတွက် အားကောင်းသော password များ အသုံးပြုခြင်း နှင့် ဖြစ်နိုင်သည့်အခါ two-factor authentication ကို အသုံးပြုခြင်းအပြင် သင့် ကွန်ပျူတာ hard-drive ကို encrpt လုပ်ရန်လည်းအရေးကြီးပါသည်။

OS X for Mac သည် File Vault 2 ဟုခေါ်သည့် သူ့ကိုယ်ပိုင် encryption ဆော့ဖ်ဝဲ နှင့် အတူ လာပါသည်။ Windows 10 သည်လည်း ပုံသေအားဖြင့် သင်၏ hard drive ကို encrypt လုပ်ပေး ထားသည်။ သို့သော် သင့်တွင် Windows ၏ အစောပိုင်း version များရှိပါက ထိုတူညီသော အရာကိုပဲ ပြုလုပ်ပေးရန် Bitlocker [20] encryption software ကို download ချယူ နိုင်ပါသည်။ သင်၏ ဖိုင်များကို PGP [21] သုံးပြီး ကိုယ်တိုင်ကိုယ်ကျ encrypt လုပ်ရန်လည်း ဆုံးဖြတ် နိုင်ပါသည်။

သင်၏ ကိရိယာ အခိုးခံရသည့်အခါ သို့မဟုတ် ပျောက်ဆုံးသည့်အခါ သင်၏ အချက်အလက်များကို လုံးဝဆုံးရှုံးသွားနိုင်ပါသည်။ ထိုအဖြစ်ကို ရှောင်ရှားရန် အလားတူ encrypt လုပ်ထားပြီးသား ဖြစ်သော external hard-drive အပေါ်တွင် သင်၏အချက်အလက်ကို အရန်သိုလှောင်ပြီး back up လုပ်ထားရန် အကြံပြုထားပါသည်။ External hard-drive သည်လည်း အခိုးခံရခြင်း သို့မဟုတ် ပျောက်ဆုံးနိုင်ခြင်း ရှိသဖြင့် တတိယ နှင့် နောက်ဆုံး ကာကွယ်ရေး နည်းလမ်းအဖြစ် ဖိုင်များကို encrypt လုပ်ထားသော cloud အပေါ်တွင် သိမ်းဆည်းထားနိုင်သည်။ Cloud storage service အတော်များများသည် Dropbox နှင့် Google Drive ကဲ့သို့ အလုပ်လုပ်သော်လည်း ၎င်းတို့သည် encryption တပါတည်း ပါဝင်ပြီးဖြစ်သဖြင့် လုံခြုံရေးပို၍မြင့်မားသည်။ အကြံပြုချက်အချို့တွင် အောက်ပါတို့ပါဝင်သည်။ -

[19] Noah Kelly, A DIY Guide to Feminist Cyber Security. Available at: https://hackblossom.org/cybersecurity/#tails. A full list of Tails' vulnerabilities can be found at: https://tails.boum.org/doc/about/warning/index.en.html.

[20] Chris Hoffman, How to Set Up BitLocker Encryption on Windows, How-To Geek, 5 October 2017. Available at: https://www.howtogeek.com/192894/how-to-set-up-bitlocker-encryption-on-windows/.

[21] For a more detailed discussion of hardware encryption, a useful article from a digital expert is: Micah Lee, Encrypting Your Laptop Like you Mean It, The Intercept, 27 April 2015. Available at: https://theintercept.com/2015/04/27/encrypting-laptop-like-mean/#osx.

- SpiderOak
- Tresorit
- Mega

သင်၏ အကြောင်းအရာအချို့သည် သင်အသုံးပြုနေသည့် မည်သည့်ကိရိယာအတွက်ပဲဖြစ်ဖြစ် ဒစ်ဂျစ်တယ်နည်းဖြင့် မှတ်တမ်းတင်ရန် သို့မဟုတ် သိမ်းဆည်းထားရန် ထိရှလွယ်လွန်းသည်ဟု အလေးအနက် စဉ်းစားရန်လည်း ဖြစ်လာနိုင်သည်။ ထို့အပြင် သင်၏ ကိရိယာများ အားလုံးမှ ဒစ်ဂျစ်တယ် ပုံစံဖြင့်မလိုအပ်သည့် အရေးကြီးသော အကြောင်းအရာများကို အမြဲတစေ ဖျက်ပစ်ရပါမည်။

ဥပမာအနေဖြင့် နယ်စပ်ဖြတ်ကျော်သည့်အခါ သို့မဟုတ် အခြားတစ်နေရာရာတွင် သိမ်းယူခံရခြင်းကဲ့သို့ ကိရိယာဖြင့် ယာယီ ခွဲခွာရပြီးနောက် ၎င်းကို တစ်စုစု ပြုပြင်ထားမည်ကို စိုးရိမ်လျှင် operating system ကို ပြန်၍ တပ်ဆင်ထည့်သွင်းခြင်း အပါအဝင် ကိရိယာကို အရန်သိုလှောင်မှု backup မှ နဂိုအတိုင်း ပြန်၍ restore လုပ်ခြင်းသည် အကြံကောင်း တစ်ခုဖြစ်သည်။ စမတ်ဖုန်းတစ်လုံး အတွက်ဆိုလျှင် အခြေအနေ နှင့် ကြုံတွေ့နိုင်သည့် အန္တရာယ်အဆင့်အပေါ် မူတည်ပြီး ဖုန်းကို စွန့်ပစ်လိုက်ပြီး အချက်အလက်ကို backup တစ်ခုမှ ရွှေ့ပြောင်းယူနိုင်သည့် ဖုန်းအသစ်တစ်လုံးဖြင့် အစားထိုးရန်ပင် စဉ်းစားနိုင်သည်။

၈။ ဖုန်း အကာအကွယ်

စမတ်ဖုန်းများသည် နည်းလမ်းပေါင်းစုံဖြင့် ထိခိုက်ပေါက်ကြားနိုင်သည်။ လူမှုမီဒီယာ များစွာက အသုံးပြုသည့် စမတ်ဖုန်းအတွင်း ပါဝင်သော GPS လုပ်ဆောင်ချက်သည် သင်၏ တည်နေရာကို ပေါက်ကြားစေနိုင်သည်။ သင့်ဖုန်း၏ Wi-Fi ကို ဖွင့်ထားခြင်းသည်လည်း တိုက်ခိုက်မှုအတွက် ထိခိုက်ခံစားလွယ်သော ပျော့ကွက်ဖြစ်သည်။ Hacker တစ်ဦးသည် အနီးမှ network တစ်ခုကို အသုံးပြုပြီး သင်က အွန်လိုင်းအပေါ်တွင် လှုပ်ရှားတက်ကြွမှု မရှိသည့်အခါမှာပင် သင်၏ metadata များ စုဆောင်းယူနိုင်သည်။ ရလဒ်အဖြစ် မလိုအပ်သည့်အခါတွင် သင့်ဖုန်းပေါ်မှ Wi-Fi နှင့် location setting တို့ကို ပိတ်ထားခြင်းက အကောင်းဆုံး ဖြစ်သည်။

သင်၏စမတ်ဖုန်းအတွင်းပါဝင်သော အကြောင်းအရာကို ကာကွယ်ရန် အကောင်းဆုံးနည်းမှာ ၎င်းကို encrypt လုပ်ရန် နှင့် အမည်မသိ browse လုပ်ရန် လိုအပ်သော ကိရိယာများ ကို download ချရန် ဖြစ်သည်။

a) Mobile Browsing Privacy

Desktop browser များမှာကဲ့သို့ iOS နှင့် Android ကိရိယာနှစ်မျိုးစလုံးအတွက် ရရှိနိုင်ပြီး Mozilla Firefox မှ ဖော်ထုတ်ထားသည့် mobile browser ကို download ချ၍ အသုံးပြုရန် အကြံပြုထားပါသည်။ Android ကိရိယာများအပေါ်တွင် Firefox mobile browser သည် အထက်တွင်ဆွေးနွေးခဲ့သော privacy extensions များအားလုံး တပ်ဆင်ထည့်သွင်းရန်လည်း ခွင့်ပြုပါသည်။ Apple ကိရိယာများအပေါ်တွင် Firefox mobile browser သည် ခြေရာခံလိုက်သူများ ၊ကြော်ငြာရှင်များကို ပိတ်ဆို့တားဆီးပေးပြီး စောင့်ကြည့်ထောက်လှမ်းခြင်းကို အနိမ့်ဆုံးဖြစ်အောင် လျှော့ချပေးရုံမက ၎င်း၏ privacy ဆိုင်ရာ လုပ်ဆောင်နိုင်စွမ်းများကို သင့် ကိရိယာပေါ်ရှိ အခြား app များဆီသို့ ဖြန့်ကျက်ခွင့်ပြုသည်။ [22]

သင်၏ ကိရိယာပေါ်ရှိ လုံခြုံမှုပိုနည်းသည့် ပုံသေပေးထားသော browser မှတစ်ဆင့် ဝက်ဘ်ဆိုက်များသို့ log in ဝင်မည့်အစား ထို ဝက်ဘ်ဆိုက်များအတွက် ဖန်တီးပေးထားသည့် တရားဝင် mobile application များကို အသုံးပြုခြင်းက ပိုကောင်းပါသည်။

b) Secure Mobile Messaging

စမတ်ဖုန်းမှတစ်ဆင့် လုံခြုံသော message ပေးပို့ခြင်းအတွက် ထိပ်ဆုံးမှ အကြံပြုထားသော ကိရိယာမှာ Signal ဟုခေါ်သည့် open source software application ဖြစ်သည်။ Signal သည် end-to-end encrypt လုပ်ထားသော ဖုန်းခေါ်ဆိုမှု နှင့် စာသား ၊ ဗီဒီယို နှင့် ရုပ်ပုံများ message ပေးပို့ခြင်း ကို ပေးကမ်းထားသည်။ ၎င်းသည် ပို့ဆောင်သည့် အကြောင်းအရာကို အပြည့်အဝ encrypt လုပ်ပေးသဖြင့် cellular network ကိုစောင့်ကြည့်ထောက်လှမ်းခြင်း ပြုလုပ်နေသည့် မည်သူမဆို စာသားအားမည်သူက ပို့ဆောင်ပြီး မည်သူက လက်ခံရရှိသည် ၊ မည်သည့်အချိန်မှာ ပို့ဆောင်သည် စသည်တို့ကို မြင်နိုင်သော်လည်း မည်သည်အရာကို ပို့ဆောင်သည်ကို မမြင်နိုင်ပါ။ WhatsApp messaging application သည်လည်း end-to-end encryption ကို ပေးကမ်းသော်လည်း Signal ၏ ထပ်ဆောင်းအကျိုးကျေးဇူးမှာ သင်၏ message များကို သင့်ဖုန်း အပေါ်ရှိနေသည့် နေရာမှာတွင်လည်း encrypt လုပ်ပေးထားခြင်းဖြစ်သည်။ သို့မှသာ အခြားတစ်ယောက်ယောက်က သင့်ဖုန်းအပေါ် ထိန်းချုပ်မှု ရရှိသွားလျှင်လည်း သိုလှောင်ထားသော message များကို ကြည့်ရှုရန် သင်၏ application နှင့် သင်၏ ဖုန်းနှစ်ခုစလုံးကို decrypt လုပ် ဝှက်စာဖော်ရန် လိုအပ်ပါလိမ့်မည်။ EFF က Android [23] နှင့် iOS [24] ကိရိယာ နှစ်မျိုးစလုံးအတွက် Signal အား

---

[22] Noah Kelly, A DIY Guide to Feminist Cyber Security, explains: "To enable these features in Safari, go to Safari under Settings, click 'Content Blockers', and enable Firefox Focus". See: https://hackblossom.org/cybersecurity/#mobilebrowsing.

[23] EFF, Surveillance-Self Defense: How to: Use Signal for Android. Available at: https://ssd.eff.org/en/node/93/.

[24] EFF, Surveillance-Self Defense: How to: Use Signal on iOS. Available at: https://ssd.eff.org/en/module/how-use-signal-ios.

မည်သို့ တပ်ဆင်ထည့်သွင်းပြီး မည်သို့ အသုံးပြုရမည်ဆိုသည်ကို ညွှန်ကြားချက်များပေးထား ပါသည်။

c) Mobile Device Encryption

အပြုသဘောဆောင်သော ဖွံ့ဖြိုးတိုးတက်မှု တစ်ရပ်မှာ ကိုယ်ပိုင်လွတ်လပ်ခွင့်ဆိုင်ရာ ပူပန်မှုများကြောင့် Apple နှင့် Android ကိရိယာ ထုတ်လုပ်သူများဘက်မှ ပုံသေအားဖြင့် သူတို့၏ ကိရိယာများကို encrypt လုပ်ပေးထားပြီး ဖုန်းအပေါ်တွင် ပါဝင်သည့် အကြောင်းအရာကို hacker များရန်မှ လုံခြုံစေရန် ဆောင်ရွက်ဖို့ အခြေအနေသို့ ဆိုက်ရောက်စေခဲ့ခြင်းဖြစ်သည်။ ထို့အပြင် ကိရိယာများသည် ယခုအခါ passcodes [25] သို့မဟုတ် လက်ဗွေရာ Touch ID သုံးစွဲခြင်းမှ တစ်ဆင့် ပို၍ မြင့်မားသော လုံခြုံရေး အဆင့်ကို ပေးကမ်းထားပါသည်။ လတ်တလောအကျဆုံး အနေဖြင့် သင်၏ ကိရိယာ ပျောက်ဆုံးသည့်အခါ သို့မဟုတ် အခိုးခံ ရသည့်အခါ အခြားသူများ ဝင်ရောက်ခြင်းမှ ထိန်းသိမ်းထားရန် Apple က မျက်နှာမှတ်သား သိရှိမှု ရွေးချယ်စရာ တစ်ခု ကိုလည်း ဖော်ထုတ်ထားပြီး ဖြစ်သည်။ Password များနည်းတူ passcode ကို စာလုံးခြောက်လုံး သို့မဟုတ် ထိုထက်ရှည်အောင်သုံးဖို့ အကြံပြုထားသည်။

EFF သည် how to best encrypt your iPhone [26] တွင် နက်နဲသော လမ်းညွှန်မှုကို ပေးထားပြီး Android [27] ကိရိယာများအတွက် Android blog Greenbot ကအလားတူ ပြုလုပ်ပေးထားသည်။

၉။ အခြားရင်းမြစ်များ နှင့် ဒစ်ဂျစ်တယ် လမ်းညွှန်များ

- EFF, Surveillance Self-Defence

  ဤလမ်းညွှန်သည် အွန်လိုင်းလုံခြုံရေး အကြောင်း ထူးကဲကောင်းမွန်သည့် အထွေထွေ ရင်းမြစ်တစ်ခုဖြစ်ပြီး ဒစ်ဂျစ်တယ် စောင့်ကြည့်ထောက်လှမ်းမှုအကြောင်း အခြေခံ ခြုံငုံသုံးသပ်မှု နှင့် ၎င်းကို ရှောင်ရှားရန် နည်းလမ်း ၊ အကူအညီရသည့် ကိရိယာများ နှင့် ဆော့ဖ်ဝဲများ တပ်ဆင်ထည့်သွင်းရန် တစ်ဆင့်ချင်း ရှင်းပြမှုများနှင့် အထူးသီးသန့် အခြေအနေများ အတွက် အသေးစိတ် လမ်းညွှန်ချက်များ ဖော်ပြထားသည်။

---

25 Passcodes are a string of characters that function as passwords do but which are specifically designed to gain access to a mobile device such as a tablet or smartphone.
26 EFF, Surveillance-Self Defense: How to: Encrypt Your iPhone. Available at: https://ssd.eff.org/en/module/how-encrypt-your-iphone.
27 Patrick Nelson, How to turn on Android encryption today (no waiting necessary), Greenbot, 19 September 2014. Available at: https://www.greenbot.com/article/2145380/why-and-how-to-encrypt-your-android-device.html.

- Committee to Protect Journalists, CPJ Journalist Security Guide: Covering the News in a Dangerous and Changing World

  ဤလမ်းညွှန်၏ 'Technology Security' အပိုင်းသည် ဆက်သွယ်ရေးကို အကာအကွယ်ပေးသည့်အခါ နှင့် အချက်အလက်ကို လုံခြုံစေသည့်အခါ စာနယ်ဇင်း သမားများ ရင်ဆိုင်နေရသည့် ခြိမ်းခြောက်မှုများကို နားလည်ရန် အကြံ ပေးထားသည်။

- Tactical Technology Collective and Front Line Defenders: Security in-a-Box – Digital Security Tools and Tactics

  ဤ ဒစ်ဂျစ်တယ် လုံခြုံရေး လမ်းညွှန်သည် ဒစ်ဂျစ်တယ်လုံခြုံရေး၏ အခြေခံ သဘောတရားများကို အနှစ်ချုပ်ဖော်ပြထားပြီး မရှိမဖြစ် အလိုအပ်ဆုံး ဒစ်ဂျစ်တယ် လုံခြုံရေး ဆော့ဖ်ဝဲ နှင့် ဝန်ဆောင်မှုများ တပ်ဆင်ထည့်သွင်းပြီး အသုံးပြုရန် အဆင့်လိုက် လမ်းညွှန်ချက်များ ပေးကမ်းထားသည်။ ၎င်းသည် အထူးသီးသန့် အုပ်စုများ အတွက် သူတို့ချဉ်းသာ သီးသန့်ရင်ဆိုင်ရသည့် ဒစ်ဂျစ်တယ် ခြိမ်းခြောက်မှုများမှ သူတို့ကိုယ်သူတို့ ကာကွယ်ရန် နည်းလမ်းကို အကြံပေးသည့် လိုအပ်ချက်နှင့် ကိုက်ညီအောင် ပြုလုပ်ထားသော 'Community Guides' ကိုလည်း ပေးကမ်းထားပါသည်။ ဤလမ်းညွှန်ချက်များသည် ထိုအထူးအုပ်စုများအတွက် လိုအပ်ချက်များ နှင့် သက်ဆိုင်ရာ ကိရိယာများ နှင့် နည်းစနစ်များအပေါ် လိုအပ်သလို ကိုက်ညီအောင် ပြုလုပ်ထားသည့် အကြံပါဝင်သည်။ (ဥပမာ , Guide for LGBT activists in Sub-Saharan Africa)

- Privacytools.io

  ဤ ဝက်ဘ်ဆိုက်သည် တစ်ကမ္ဘာလုံးဆိုင်ရာ အုံလိုက်ကျင်းလိုက် စောင့်ကြည့်ထောက်လှမ်းခြင်းအကြောင်း သတင်းအချက်များ ဖော်ပြထားပြီး ၎င်းတို့ကို ကာကွယ်ရန် VPN provider များ ၊ browser testing tool များ နှင့် add-on များ စာရင်းကဲ့သို့ ကိရိယာများအကြောင်း ဖော်ပြထားသည်။

- We Fight Censorship, Online Survival Kit

  ဤလမ်းညွှန်က"ဆင်ဆာဖြတ်တောက်မှုကိုကျော်လွှားရန် နှင့် သင်၏ ဆက်သွယ်ရေးများ နှင့် အချက်အလက်ကို လုံခြုံစေရန် နည်းလမ်းများအား သင့်ကို သင်ကြားပေးရန် လက်တွေ့ အသုံးပြုနိုင်သည့် ကိရိယာများ ၊ အကြံဉာဏ် နှင့် နည်းစနစ်များ ပေးကမ်းထားပြီး " စာဖတ်သူအား "သတင်း နှင့် အကြောင်းအရာအချက်အလက်များ

ထိန်းချုပ်လိုပြီး သဘောထားကွဲလွဲသည့်အသံများ ပိတ်ပင်တားဆီးလိုသည့် ဆင်ဆာများ ၊ အစိုးရများ သို့မဟုတ် အထူးစိတ်ဝင်စားမှုရှိသည့် အုပ်စုများ ကို တွန်းလှန်ရန် နည်းလမ်းနှင့်အတူ ” ထောက်ပံ့ပေးရန် ရည်ရွယ်ပါသည်။

- Digitaldefenders.org, Digital First Aid Kit

  ဤလမ်းညွှန်သည် “ ဒစ်ဂျစ်တယ်ခြိမ်းခြောက်မှု၏ အတွေ့ရအများဆုံးပုံစံ ကို ရင်ဆိုင်နေရသူများ အတွက် ကနဦးအထောက်အပံ့ပေးရန် ရည်ရွယ်သည်။ Kit သည် လူ့အခွင့်အရေး ကာကွယ်သူများ ၊ ဘလော့ဂ်ဂါများ ၊ လှုပ်ရှားတက်ကြွသူများ နှင့် သူတို့ ကိုယ်တိုင် တိုက်ခိုက်မှုများ နှင့် ရင်ဆိုင်နေရသည့် စာနယ်ဇင်းသမားများအတွက် ကိုယ်တိုင်ပြစ်ချက်ရှာ ကိရိယာများ အစုံလိုက် ပေးကမ်းပြီး ခြိမ်းခြောက်ခံနေရသူ လူပုဂ္ဂိုလ်တစ်ဦးအတွက် ကူညီပေးရန် ဒစ်ဂျစ်တယ်ဆိုင်ရာ ရှေ့ပြေးတပ်ဖွဲ့ - first responder များ အတွက် လမ်းညွှန်ချက်များ ထောက်ပံ့ပေးပါသည် ”

- Hack*Blossom, A DIY Guide to Feminist Cybersecurity

  ဤလမ်းညွှန်သည် “ ရနိုင်သမျှ တန်ဖိုးအရှိဆုံးဆိုင်ဘာလုံခြုံရေးကိရိယာအချို့ အတွက် ပြည့်စုံလွှမ်းခြုံပြီး ဖတ်ရှုနားလည်နိုင်သော မိတ်ဆက်အညွှန်းတစ်ခု ဖြစ်ရန်” ရည်ရွယ်သည်။ လမ်းညွှန်က အွန်လိုင်းအမည်မသိ လှုပ်ရှားရှင်သန်မှုကို ထိန်းသိမ်းရန် ၊ hack အလုပ်ခံရခြင်းမှ ရှောင်ရှားရန် နှင့် အွန်လိုင်း နှင့် ကိရိယာအမျိုးအစား အားလုံးအပေါ်မှ အချက်အလက် ကာကွယ်ရန်တို့အတွက် နည်းလမ်းအပေါ် အကြံပေးထားပါသည်။

၁၀။ နည်းပညာဝေါဟာရ [28]

Add-on

“အခြားအသုံးချဆော့ဖ်ဝဲ တစ်ခုကို ပြုပြင်မွမ်းမံပြီး ၎င်းအလုပ်လုပ်ပုံ သို့မဟုတ် ၎င်းပြုလုပ်နိုင်သည့်အရာကို ပြောင်းလဲပေးသော ဆော့ဖ်ဝဲ အစိတ်အပိုင်း တစ်ခု။ Add-on များသည် မကြာခဏဆိုသလို web browser သို့မဟုတ် အီးမေးလ် ဆော့ဖ်ဝဲတို့တွင် ကိုယ်ပိုင်လွတ်လပ်ခွင့် သို့မဟုတ် လုံခြုံရေးဆိုင်ရာ လုပ်ဆောင်မှုများ ပေါင်းထည့်ပေးနိုင်သည်။ အချို့သော add-on များသည် အဖျက်အမှောင့်ပြုသော malware များဖြစ်သဖြင့်

[28] The definitions in this glossary are all taken from the Electronic Frontier Foundation's Surveillance Self-Defence Glossary. Available at: https://ssd.eff.org/en/glossary.

နာမည်ကောင်းရှိပြီး တရားဝင်ရင်းမြစ်မှရသည့် add-on များကိုသာ install လုပ်ရန် ဂရုစိုက်သင့်သည်။"

Commercial VPN

"စီးပွားဖြစ် Virtual Private Network တစ်ခုသည် သင်၏ အင်တာနက် ဆက်သွယ်ရေးများကို သူတို့ကိုယ်ပိုင် network မှတစ်ဆင့် လုံခြုံစွာ လက်ဆင့်ကမ်း ပို့ဆောင်မှုကို ပေးကမ်းသည့် ပုဂ္ဂလိက ဝန်ဆောင်မှု တစ်ခုဖြစ်သည်။ ထိုသို့ပြုလုပ်ခြင်းအတွက် အကျိုးကျေးဇူးမှာ သင် ပို့လွှတ်သမျှ နှင့် လက်ခံသမျှ အချက်အလက်များ အားလုံးကို ဒေသခံ network များမှ ကွယ်ဝှက်ပေးထားခြင်းဖြစ်သည်။ ထို့ကြောင့် အနီးအနားမှ ဒုစရိုက်သမားများ သို့မဟုတ် ယုံကြည်စိတ်ချရခြင်း မရှိသည့် ဒေသခံ ISP များ သို့မဟုတ် ဆိုင်ဘာကဖေးများ၏ ရန်မှ ပို၍ဘေးကင်းပါသည်။ VPN တစ်ခုသည် ပြင်ပနိုင်ငံ တစ်ခုတွင် အခြေစိုက်နိုင်ပြီး ဒေသခံအစိုးရထံမှ ဆက်သွယ်မှုများကို ကာကွယ်ရန် နှင့် အမျိုးသားအဆင့် ဆင်ဆာဖြတ်တောက်မှုကို ရှောင်ကွင်းကျော်ဖြတ်ရန် နှစ်ခုစလုံးအတွက် အသုံးဝင်ပါသည်။ အားနည်းချက်မှာ ကွန်ရက်အပေါ်သွားလာမှု အများစုကို စီးပွားဖြစ် VPN ၏ အစွန်းပိုင်းတွင် decrypt လုပ်ခြင်း ဖြစ်သည်။ ဆိုလိုသည်မှာ သင်၏ အွန်လိုင်းအပေါ် သွားလာမှုကို စီးပွားဖြစ် VPN (နှင့် ၎င်းတည်ရှိသည့်နိုင်ငံ) က ခိုးယူကြည့်ရှုမှု မပြုကြောင်း ယုံကြည်စိတ်ချရဖို့ လိုအပ်ပါသည်။"

Cookies

"Cookies သည် ဝက်ဘ်ဆိုက်များက သင်၏ browser ကို မှတ်မိနေစေရန် ခွင့်ပြုသည့် ဝက်ဘ်နည်းပညာ တစ်ခုဖြစ်သည်။ Cookies များသည် မူလအစက ဝက်ဘ်ဆိုက်များ အနေဖြင့် အွန်လိုင်းဈေးဝယ်လှည်းများ ပေးကမ်းရန်၊ စိတ်ကြိုက် ရွေးချယ်မှုများ သိမ်းဆည်းထားရန် သို့မဟုတ် ဝက်ဘ်ဆိုက် တစ်ခုသို့ log on ဝင်ရောက်မှုအား ဆက်ထိန်းထားရန် ဖြစ်နိုင်စေရေးအတွက် ပုံစံထုတ်ထားသည့် ဝက်ဘ်နည်းပညာတစ်ခု ဖြစ်သည်။ ၎င်းတို့သည် ခြေရာခံခြင်း နှင့် လူပုဂ္ဂိုလ် အခြင်းအရာ ကောက်ကြောင်း ဖော်ယူခြင်းကို စွမ်းဆောင်နိုင်ပြီး ထို့အတွက်ကြောင့် ဝက်ဘ်ဆိုက်များသည် သင့်ကိုမှတ်မိနိုင်မည်။ "သင်ဘယ်ကို သွားသည်။ မည်သည့် ကိရိယာကို သုံးစွဲသည်။ မည်သည့် အကြောင်းအရာကို စိတ်ဝင်စားသည်။" စသည်ဖြင့် ပိုမိုသိရှိနိုင်မည်။ ထို ဝက်ဘ်ဆိုက်တွင် သင့်၏ account မရှိလျှင်တောင်မှ သို့မဟုတ် log in ဝင်မထားသည့် အခါမှာတောင်မှ ထိုသို့ သိရှိနိုင်ပါသည်။ "

Cryptography

"သတင်းစကားများကို အခြားမသက်ဆိုင်သူများက နားလည်နိုင်စွမ်း မရှိဘဲ လက်ခံသူထံ ပို့လွှတ်ရန် နှင့် လက်ခံရယူရန် လျှို့ဝှက်ကုဒ်များ သို့မဟုတ် ဝှက်စာစနစ်များ ပုံစံထုတ်ခြင်း အတတ်ပညာ"

Decrypt

"လျှို့ဝှက်သတင်းစကားတစ်ခု သို့မဟုတ် အချက်အလက်ကို နားလည်နိုင်အောင် ဖော်ယူသည်။ Encryption ပြုလုပ်ခြင်းနောက်ကွယ်မှ စိတ်ကူးအကြံအစည်သည် လက်ခံရရှိရန် ရည်ရွယ်ထားသည့် လူပုဂ္ဂိုလ် သို့မဟုတ် လူအုပ်စုသာ decrypt လုပ် အဓိပ္ပါယ် ဖော်ယူနိုင်မည့် သတင်းစကားများ ဖန်တီးရန် ဖြစ်သည်။ "

Encrypt

"သတင်းအချက်အလက် သို့မဟုတ် ဆက်သွယ်ရေး မည်သည့် ပုံစံမျိုး အတွက်မဆို encryption နည်းပညာ အသုံးချသည်။ ဤနည်းလမ်းတွင် သတင်းအချက်အလက် သို့မဟုတ် ဆက်သွယ်ရေးကို အဓိပ္ပါယ်မရှိသည့် ပုံပေါက်အောင် ပုံစံပြောင်းပေးသည့်တိုင် မှန်ကန်သည့် လျှို့ဝှက်သော့ချက်ရှိသည့် လူပုဂ္ဂိုလ် သို့မဟုတ် ကိရိယာက မူလပုံစံ အတိုင်း ပြန်လည်ပြီး ဖော်ယူနေနိုင်ဆဲဖြစ်အောင် ပြုလုပ်ထားသည်။ ဤအစီအစဉ်က သတင်းအချက်အလက်အားမည်သူက ရယူသုံးစွဲနိုင်သည်ကို ကန့်သတ်ထားသည်။ အဘယ်ကြောင့် ဆိုသော် မှန်ကန်သည့် လျှို့ဝှက်သော့ချက်မရှိလျှင် encryption ကို ပြောင်းပြန်လုန်ပြီး မူလသတင်းအချက်အလက် ပြန်ရအောင် ပြုလုပ်ရန် မဖြစ်နိုင်သည့်အတွက်ပင် ဖြစ်သည်။ Encryption သည် cryptography ခေါ်သည့် ပညာရပ် နယ်ပယ် အတွင်း ဖွဲ့စည်းပါဝင်သည့် နည်းပညာများစွာထဲမှ တစ်ခုဖြစ်သည်။ "

End-to-end encryption

"End-to-end encryption က သတင်းစကားတစ်ခုကို ၎င်း၏ မူလပို့ဆောင်သူက လျှို့ဝှက်သတင်းစကားတစ်ခုအဖြစ် ပြောင်းပေးပြီး ၎င်း၏ နောက်ဆုံးလက်ခံရရှိသူကသာ အဓိပ္ပါယ်ပြန်ဖော်ယူကြောင်း သေချာစေသည်။ Encryption ၏ အခြားပုံစံများသည် တတိယအဖွဲ့က လုပ်ဆောင်သည့် encryption အပေါ်မှီခိုနေရနိုင်သည်။ ထိုသို့ဖြစ်သည့်အတွက် မူရင်းစာသား နှင့် ပတ်သက်၍ ထိုအဖွဲ့များသည် ယုံကြည်စိတ်ချရမှု ရှိဖို့ လိုအပ်သည်။ End-to-end encryption သည် encryption ကို ကြားဝင်နှောင့်ယှက်ရန် သို့မဟုတ် ချိုးဖောက်ရန် စွမ်းရည်ရှိသည့် အဖွဲ့များ၏ အရေအတွက်ကို လျှော့ချပေးသဖြင့် ယေဘုယျအားဖြင့် ပို၍ ဘေးကင်းသည်ဟု မှတ်ယူထားကြသည်။ "

Key

"Cryptography တွင် သင့်အား သတင်းစကားတစ်ခုကို encrypt လုပ်ရန် သို့မဟုတ် decrypt လုပ်ရန် စွမ်းရည်ကိုပေးသည့် အချက်အလက် အပိုင်းအစတစ်ခုဖြစ်သည်။"

Malware

"Malware ဟူသည် malicious software အတွက် အတိုကောက်စကားလုံးဖြစ်သည်။ ၎င်းမှာ သင်၏ ကိရိယာအပေါ်တွင် မလိုလားအပ်သည့် လှုပ်ရှားမှုများ ဆောင်ရွက်ရန် ပုံစံထုတ်ထားသည့် ပရိုဂရမ်များ ဖြစ်သည်။ ကွန်ပျူတာဗိုင်းရပ်စ်များသည် malware ဖြစ်သည်။ Password များ ခိုးယူသည့် ပရိုဂရမ်များ၊ သင့်ကို လျှို့ဝှက်စွာ အရုပ်အသံ ဖမ်းယူရိုက်ကူးသည့် ပရိုဂရမ် သို့မဟုတ် သင်၏ အချက်အလက်ကို ဖျက်ပစ်သည့် ပရိုဂရမ် များသည်လည်း malware ပင်ဖြစ်သည်။ "

Metadata

" Metadata(သို့မဟုတ်"အချက်အလက်အကြောင်းအချက်အလက်") သည် သတင်း အချက်အလက် ကိုယ်တိုင်မှလွဲ၍ ထို သတင်းအချက်အလက်နှင့် သက်ဆိုင်ရာ အကြောင်း အရာများ အားလုံးပင်ဖြစ်သည်။ ထို့ကြောင့် သတင်းစကားတစ်ခု၏ အကြောင်းအရာသည် metadata မဟုတ်ပါ။ သို့သော် မည်သူက မည်သည့်အချိန်တွင် မည်သည့်နေရာမှ မည်သူထံ ပို့ဆောင်သည် ဆိုသည့် အချက်အားလုံးမှာ metadata ၏ နမူနာများပဲ ဖြစ်ပါသည်။ တရားရေးစနစ်များသည် အခါများစွာတွင် အကြောင်းအရာ ကို metadata ထက်ပိုပြီး အကာအကွယ်ပေးကြသည်။ ဥပမာ အမေရိကန်တွင် တရားဥပဒေစိုးမိုးရေး တပ်ဖွဲ့က လူပုဂ္ဂိုလ်တစ်ဦး၏ ဖုန်းခေါ်ဆိုမှုကို နားထောင်ရန် ဝရမ်းလိုအပ်သော်လည်း သင် ဖုန်းခေါ်ဆိုခဲ့သည့်သူများစာရင်းကိုရယူရန် ရပိုင်ခွင့်ကို များစွာပို၍လွယ်ကူစွာဖြင့် တောင်းဆို နိုင်သည်။သို့သော် metadata သည် အခါများစွာတွင် အကြောင်းအရာများစွာကို ဖော်ထုတ် လုစ်ဟပြနိုင်ပြီး ၎င်းကဖော်ပြသည့် အချက်အလက်နည်းတူ ဂရုတစိုက်ဖြင့် အကာအကွယ် ပေးရန် လိုအပ်ပါသည်။ "

Online harassment

"ထိခိုက်စော်ကားသည့် အမည်ဖြင့် အခေါ်ခံရခြင်း၊ အရှက်ခွဲရန် တမင်သက်သက် အားစိုက် ဆောင်ရွက်ခြင်း ၊ ရုပ်ပိုင်းအရ ခြိမ်းခြောက်ခံရခြင်း ၊ နောက်ယောက်ခံ အလိုက်ခံရခြင်း ၊

အဆက်မပြတ် ရှည်ကြာစွာ အနှောင့် အယှက်အပေးခံရခြင်း နှင့် လိင်ပိုင်းဆိုင်ရာအရ အနှောင့်အယှက်အပေးခံရခြင်း"[29]

Operating system

"ကွန်ပျူတာတစ်လုံးအပေါ်တွင် အခြား ပရိုဂရမ်များအားလုံးကို လည်ပတ်ပေးသော ပရိုဂရမ် တစ်ခု။ Windows, Android နှင့် Apple ၏ OS X နှင့် iOS တို့အားလုံးသည် operating system နမူနာများ ဖြစ်သည်။"

PGP

"PGP or Pretty Good Privacy သည် public key cryptography ၏ ပထမဆုံး ရေပန်းစားသောလက်တွေ့အကောင်အထည်ဖော်မှု တစ်ရပ်ဖြစ်သည်။ ၎င်းကို ဖန်တီးသူ Phil Zimmermann သည် လှုပ်ရှားတက်ကြွသူများ နှင့် အခြားသူများက သူတို့၏ အသိုင်းအဝိုင်းကို ကာကွယ်နိုင်ရန် ထို ပရိုဂရမ်ကို ၁၉၉၁ ခုနှစ်တွင် ရေးသားခဲ့သည်။ ပရိုဂရမ်သည် အမေရိကန် ပြင်ပတွင် ပျံ့နှံ့သွားသောအခါ သူသည် အမေရိကန်အစိုးရ၏ တရားဝင် စုံစမ်းစစ်ဆေးမှုကို ခံခဲ့ရသည်။ ထိုအချိန်က အားကောင်းသည့် public key encryption ပါဝင်သည့် ကိရိယာနည်းလမ်းများ ပြည်ပပို့ကုန်အဖြစ်တင်ပို့ခြင်းသည် အမေရိကန် ဥပဒေကို ချိုးဖောက်မှုပင်ဖြစ်သည်။ PGP သည် စီးပွားဖြစ်ရောင်းချသည့် ဆော့ဖ်ဝဲထုတ်ကုန် အဖြစ် ဆက်ပြီးရှိနေသည်။ PGP ကအသုံးပြုထားသည့် တူညီသော အခြေခံ စံသတ်မှတ်ချက်ကိုပဲ အခမဲ့ အကောင်အထည်ဖော်ထားသော GnuPG (or GPG) ဟုခေါ်သည့် နည်းလမ်းကိုလည်း ရရှိနိုင်သည်။ နှစ်မျိုးစလုံးသည် အပြန်အလှန်လဲလှယ်နိုင်သည့် တူညီသော ချဉ်းကပ်နည်းကိုပဲ အသုံးပြုထားသောကြောင့် လူအများသည် GnuPG ကို အသုံးပြုနေသည့်အခါမှာပင် "PGP key" တစ်ခု အသုံးပြုခြင်း သို့မဟုတ် "PGP message" ပို့ဆောင်ခြင်းဟု ရည်ညွှန်းကြပါသည်။ "

Risk analysis

"ကွန်ပျူတာ လုံခြုံရေးတွင် risk analysis ဆိုသည်မှာ ခြိမ်းခြောက်မှု အောင်မြင်နိုင်သည့် အခွင့်အလမ်းကို တွက်ချက်ခြင်းဖြစ်သည်။ သို့မှသာ ၎င်းတို့မှ ကာကွယ်ရန် မည်မျှ အားစိုက်ရမည်ကို သိရှိနိုင်မည်ဖြစ်သည်။ သင်၏ အချက်အလက်သို့ ထိန်းချုပ်မှု သို့မဟုတ် ရယူသုံးစွဲခွင့် ဆုံးရှုံးနိုင်သည့် နည်းလမ်းပေါင်း မြောက်မြားစွာရှိနိုင်ပါသည်။ သို့သော် အချို့သည် ကျန်သည့် နည်းလမ်းများထက် ဖြစ်နိုင်ခြေ ပိုနည်းပါသည်။ အန္တရာယ်အကဲဖြတ် ဆန်းစစ်ခြင်း ဆိုသည်မှာ မည်သည့် ခြိမ်းခြောက်မှုများကိုတော့ အလေးအနက်

[29] Maeve Dugan, *Online Harassment 2017,* Pew Research Center – Internet and Technology (Jul. 11, 2017), http://www.pewInternet.org/2017/07/11/online-harassment-2017/.

သဘောထားပြီး မည်သည့်အရာများကိုတော့ စိုးရိမ်ပူပန်ရန် မလိုလောက်အောင် ဖြစ်ပွားမှုရှားပါးလွန်းသည် သို့မဟုတ် ဘေးအန္တရာယ်ပြုနိုင်ခြင်းမရှိ (သို့မဟုတ် ခုခံတိုက်ခိုက်ရန် ခက်ခဲလွန်းသည်။) ဟု ဆုံးဖြတ်ခြင်းပဲ ဖြစ်ပါသည်။ Threat modeling တွင်ကြည့်ပါ။"

Threat model

" သင်၏ အချက်အလက်အတွက် သင် အကာအကွယ် ယူလိုသည့် အမျိုးအစားများ အကြောင်း ကျဉ်းမြောင်းစွာ စစ်ထုတ်ပိုင်းခြားသည့် စဉ်းစားနည်းတစ်ခု ဖြစ်သည်။ နည်းလမ်း သို့မဟုတ် တိုက်ခိုက်သူ အမျိုးအစားအားလုံး၏ ရန်မှ ကာကွယ်ရန် မဖြစ်နိုင်ပါ။ ထို့ကြောင့် သင်၏ အချက်အလက်ကို လိုချင်သည့်သူများ ၊ ၎င်းမှ သူတို့လိုချင်သည့်အရာနှင့် သူတို့ ရယူနိုင်မည့် နည်းလမ်းတို့အပေါ် အာရုံစိုက်သင့်သည်။ သင်က အကာအကွယ် ယူရန် စီမံထားသည့် ဖြစ်နိုင်ဖွယ်ရှိသော တိုက်ခိုက်မှု အစုအဝေးအား ဖော်ထုတ်ယူခြင်းကို threat modeling ဟုခေါ်သည်။ ခြိမ်းခြောက်မှု ပုံစံငယ် - threat model ကို ရရှိပြီးသည်နှင့် risk analysis တစ်ခုကို ဆောင်ရွက်နိုင်ပြီ ဖြစ်ပါသည်။"

VPN

"Virtual private network တစ်ခုသည် အင်တာနက်၏ အခြားတစ်ဘက်မှ အဖွဲ့အစည်း တစ်ခု၏ network သို့ သင်၏ ကွန်ပျူတာကို လုံခြုံစွာ ဆက်သွယ်ရန် နည်းစနစ် တစ်ခုဖြစ်သည်။ VPN တစ်ခုကို အသုံးပြုသည့်အခါ သင့်ကွန်ပျူတာ၏ ဆက်သွယ်မှု အားလုံးကို အတူတကွ သိမ်းထုတ်ပြီး encrypt လုပ်ကာ ထို အခြား အဖွဲ့အစည်းသို့ လက်ဆင့်ကမ်းပေးသည်။ ထိုနေရာတွင် decrypt လုပ်ပြီး ပြန်လည်ဖြေချကာ ၎င်း၏ ခရီးပန်းတိုင်သို့ ပို့ဆောင်ပေးသည်။ အဖွဲ့အစည်း၏ network သို့မဟုတ် ပို၍ကျယ်ပြန့်သော အင်တာနက်ပေါ်မှ အခြားမည်သည့်ကွန်ပျူတာအတွက်မဆို သင့်ကွန်ပျူတာ၏ တောင်းခံမှုသည် သင်၏ တည်နေရာမှ မဟုတ်ဘဲ အဖွဲ့အစည်းတွင်းမှ လာသည့်ပုံပေါက်နေပါသည်။ VPN များကို စီးပွားရေး လုပ်ငန်းများက ဌာနတွင်း အရင်းအမြစ်များသို့ လုံခြုံသော ရယူသုံးစွဲခွင့် ထောက်ပံ့ပေးရန် အသုံးပြုကြသည်။ (ဖိုင် server များ သို့မဟုတ် ပရင်တာများကဲ့သို့) တစ်သီးပုဂ္ဂလများကလည်း ဒေသန္တရ ဆင်ဆာဖြတ်တောက်မှုကို ကျော်လွှားရန် သို့မဟုတ်ဒေသန္တရစောင့်ကြည့်ထောက်လှမ်းမှုကိုပျက်ပြားစေရန်၎င်းကိုအသုံးပြုကြသည်။ "