လူထုဝိုင်ဖိုင်သုံးစွဲရာတွင် ဘေးကင်းစေရန် အကြံပြုချက်များ

သမာသူများအနေဖြင့် သင့်ကို အွန်လိုင်းမှတစ်ဆင့် အမြတ်ထုတ်သွားနိုင်ပါသည်။ လူထုဝိုင်ဖိုင်သုံးစွဲရန်လိုအပ်ပါက အောက်ပါအကြံပြုချက်များကို သုံးသပ်ပါ။

ကိုရိုနာဗိုင်းရပ်စ်ဖြစ်ပွားမှုကြောင့် စီးပွားရေးလုပ်ငန်းများ နှင့် စာကြည့်တိုက်များ ပိတ်သိမ်းထား၍ ကျွန်ုပ်တို့၏ အွန်လိုင်းအသုံးပြုမှုမှာ ပိုမိုများပြားလာပါသည်။ ရလဒ်အနေဖြင့် အင်တာနက်အသုံးပြုရန်အတွက် လူထုဖိုင်ဝိုင်ကို အသုံးပြုရန်လိုအပ်ကောင်းလိုအပ်လာနိုင်ပါသည်။ လူထုဝိုင်ဖိုင်အသုံးပြုရန်လိုအပ်လာပါက သင်၏အချက်အလက်များကို ကာကွယ်ရန် ကျေးဇူးပြု၍ State Chief Privacy Officer ၏ အောက်ပါတိုက်တွန်းချက်များ ကို သုံးသပ်ပါ-

1. သင့်တွင်မှန်ကန်သော ကွန်ရက်ရှိကြောင်းသေချာစေပါ။

သင်သည် မှန်ကန်သော ကွန်ရက်ကိုသာ ချိတ်ဆက်နေကြောင်း သေချာစေပါ။ မသမာသူများအနေဖြင့် သူတို့၏ကိုယ်ပိုင်အမည်များဖြင့် ဘေးကင်းပုံပေါက်သော ကွန်ရက်များကို ဖန်တီးထားနိုင်သော်လည်း အမှန်မှာ သင်၏အင်တာနက် အသုံးပြုမှုများကို ကြည့်ရှုရန်ကွန်ရက်များကို ဖန်တီးထားပြီး ၎င်းတို့ဆီသို့ပို့ဆောင်ပေးနေခြင်း ဖြစ်နေနိုင်ပါသည်။ ဆိုလိုရင်းမှာ သင်သည်သင်၏အချက်အလက်များ သို့မဟုတ် လျှို့ဝှက်ကုဒ်များကို သုံး၍ ဝက်ဘ်ဆိုက်များထဲသို့ဝင်ရောက်မိပါက ဟက်ကာများအနေဖြင့် သင်၏အချက်အလက်များကို ခိုးယူသွားနိုင်ပါသည်။ ယင်းကိုကာကွယ်နိုင်ရန်အတွက် ကွန်ရက်၏အမည်ကို ဂရုတစိုက်ဖတ်ရှုပြီး ဖြစ်နိုင်မည်ဆိုလျှင် ၎င်းကွန်ရက်မှာ တရားဝင်ဖြစ်ကြောင်းသေချာစေရန် သက်ဆိုင်ရာဝန်ထမ်းကိုမေးမြန်းပါ သို့မဟုတ် လုပ်ငန်းအမှတ်အသားကို စစ်ဆေးပါ။

လူသိများသည့်ကော်ဖီလုပ်ငန်းကဲ့သို့သောကွန်ရက် များသည် မိမိတို့၏ ကုမ္ပဏီဝန်ဆောင်မှုတစ်ခုအနေဖြင့်သာ ကွန်ရက်ကို အသုံးပြုသောကြောင့် သံသယဖြစ်စရာအကြောင်းရင်း သိပ်မရှိပါ။ လူသိများသော ကွန်ရက်များသည် လူထုနေရာများတွင် သင့်၏ဖုန်းတွင်ပေါ်လာနိုင်သော အခမဲ့ကြံ့ရာကွန်ရက်များထက် ပုံမှန်အားဖြင့် ပို၍လုံခြုံပါသည်။

2. အလိုအလျောက်ချိတ်ဆက်မှုကို ပိတ်ထားပါ။

ပစ္စည်းအတော်များများ (စမတ်ဖုန်းများ၊လက်ပ်တော့များ နှင့် တက်ပလပ်များ) တွင် အလိုအလျောက်ချိတ်ဆက်သည့် စက်တင်များပါဝင်ပါသည်။ ယင်းစက်တင်မှာ သင့်ကိရိယာများကို အနီးအနားဝန်းကျင်ရှိ ကွန်ရက်များနှင့် လွယ်ကူစွာ ဖြင့် ချိတ်ဆက်ရန် လုပ်ဆောင်ပေးပါသည်။ ၎င်းမှာ ယုံကြည်စိတ်ချရသော ကွန်ရက်များအတွက် အဆင်ပြေနိုင်သော်လည်း မလုံခြုံသည့် ကွန်ရက်များဖြင့်လည်း ချိတ်ဆက်မိသွားနိုင်သည်။ သင်၏ ကိရိယာတွင် ရှိသည့် စက်တင်မှတစ်ဆင့် ယင်းလုပ်ဆောင်မှုကို ပိတ်ထားနိုင်ပါသသည်။ အထူးသဖြင့် သင်နှင့် စိမ်းသောဝန်းကျင်များတွင် ယင်းလုပ်ဆောင်မှုစက်တင်များကို ပိတ်ထားပါ။ ပို၍ လုံခြုံစေရန်အတွက် လူထုဝိုင်ဖိုင်ကို အသုံးပြုပြီးတိုင်း “forget network” ကို အသုံးပြုပါ။

သင်၏ Bluetooth ကိုလည်း လူထုနေရာများတွင် ချိန်ညှိထားသင့်ပါသည်။ Bluetooth ချိတ်ဆက်မှုသည် တခြားသောကိရိယာများ နှင့် ဆက်သွယ်နိုင်စေရန်လုပ်ဆောင်ပေးသည့်အတွက် ပွင့်နေသော Bluetooth အချက်ပြမှုမှတစ်ဆင့် သင်၏ ကိရိယာများကို ဝင်ရောက်ထိန်းချုပ်ရန် ဟက်ကာများမှ ရှာဖွေတွေ့ရှိသွားနိုင်ပါသည်။ သင်နှင့် စိမ်းသောဝန်းကျင်များတွင် ရောက်ရှိနေပါက ယင်းလုပ်ဆောင်မှုများကို သင်၏ဖုန်း နှင့် တခြားသော ကိရိယာများတွင် ပိတ်ထားပါ။

3. ဖိုင်ရှဲခြင်းကို ပိတ်ထားပါ။

လူထုဖိုင်ဝိုင်အသုံးပြုနေစဉ်တွင် ဖိုင်ရှဲခြင်း လုပ်ဆောင်မှုကို ပိတ်ထားသည်ကို သေချာစေပါ။ သင်၏ operating system ပေါ်မူတည်၍ system preferences သို့မဟုတ် control panel မှတစ်ဆင့် ဖိုင်ရှဲခြင်းကို ပိတ်ထားနိုင်ပါသည်။ AirDrop သည် သင်ပိတ်ထားရန် လိုအပ်သည့် ဖိုင်ရှဲနိုင်သည့် လုပ်ဆောင်ချက်ပါဝင်သည့် ဥပမာတစ်ခုဖြစ်ပါသည်။ Windows/PC ကဲ့သို့သော operating system များတွင် ကွန်ရက်အသစ်သို့ ပထမဦးအကြိမ် ချိတ်ဆက်ရာတွင် “public” ဟူ၍ ရွေးချယ်ထားပေးပါက ဖိုင်ရှဲခြင်း လုပ်ဆောင်ချက် ကို ပိတ်ထားပေးပါလိမ့်မည်။

ဖိုင်ရှဲခြင်းကို ပိတ်ရန်အဆင့်များ

PC တွင်-

1. Network and Sharing Center သို့ သွားပါ။
2. ပြီးလျှင် advanced sharing settings ကိုပြောင်းပါ။
3. ပရင်တာ နှင့် ဖိုင်ရှဲခြင်းကို ပိတ်လိုက်ပါ။

Macs တွင်-

1. System Preferences သို့သွားပါ။
2. Sharing ကိုရွေးပါ။

3. ရွေးချယ်ထားသည့်အရာ အားလုံးကို ပြန်ဖြုတ်ပါ။
4. ပြီးနောက် Finder တွင် AirDrop ကို နှိပ်ပါ ၊ ပြီးလျှင် ကျွန်ုပ်ကို ရှာဖွေခွင့်ပြုထားသူများတွင်- မည်သူကိုမျှကို ရွေးပါ။

iOS တွင်၊ Control Center တွင် AirDrop ကိုရှာ၍ ပိတ်လိုက်ပါ။

4. VPN သုံးပါ။

သင်၏ ကိရိယာတွင် VPN (အဝေးထိန်းကိုယ်ပိုင်ကွန်ရက်) ကို တပ်ဆင်ရန် သုံးသပ်ပါ။ VPN ဆိုသည်မှာ လူထုပိုင်ဖိုင်တွင် ဒီဂျစ်တယ်သီးသန့် အသုံးပြုမှုအတွက် လုံခြုံစိတ်ချရသည့် လုပ်ဆောင်မှုတစ်ခု ဖြစ်ပါသည်။ ယင်းသည် သင်၏ကိရိယာမှ ဖြတ်သွားသောအချက်အလက်များ နှင့် ဝင်လာသောအချက်အလက်များကို "လိုဏ်းခေါင်း" သဖွယ်ကာကွယ်ပြောင်းလဲပေးသဖြင့် ကွန်ရက်အတွင်းသို့ ဝင်ရောက်သော်လည်း သင်၏ အချက်အလက်များကို မြင်တွေ့နိုင်စွမ်းမရှိစေတော့ပါ။

5. FBI မှ သတိပေးထားသည့် ပြုပြင်ပြောင်းလဲထားသော ဝက်ဘ်ဆိုက်များ – HTTPS

FBI မှ "https"ဖြင့်အစပြုသော ဝက်ဘ်ဆိုက်လိပ်စာများကို သတိပေးထားပါသည်။ "https" ပါရှိနေခြင်း နှင့် သော့ခတ်ထားသောအမှတ်အသားက web traffic သည်အချက်အလက်များကို ပြုပြင်ပြောင်းလဲထားပြီး ဝင်ရောက်ကြည့်ရှုသူများ အနေဖြင့် မိမိတို့၏ အချက်အလက်များကို လုံခြုံစွာ ဝေမျှနိုင်ကြောင်း ဖော်ပြထားခြင်း ဖြစ်သည်။ သို့သော်လည်း ဆိုက်ဘာသမားသူများအနေဖြင့် ယခုအခါတွင် လုံခြုံသယောင်ရှိသော်ငြား မလုံခြုံသည့် https ပါဝင်သည့် သံသယဖြစ်ဖွယ်ဝက်ဘ်ဆိုက်များ အားဖြင့် လူအတော်များများကို သွေးဆောင်ဖြားယောင်း၍ လူထု၏ ယုံကြည်မှုကို ရရှိအောင်လုပ်ဆောင်နေပါသည်။

FBI ၏ တိုက်တွန်းချက်-

- အီးမေးလ်တွင်ပါသည့် အမည်ကို အလွယ်တကူမယုံကြည်ပါနှင့်-အီးမေးလ်တွင် ပါဝင်သည့် အကြောင်းအရာ၏ ရည်ရွယ်ချက်ကို မေးမြန်းပါ။
- မိမိသိရှိသည့်သူထံမှ သံသယဖြစ်ဖွယ် အီးမေးလ် နှင့် လင့်ခ်ကို လက်ခံရရှိပါက အချက်အလက်သည် စစ်မှန်ကြောင်း ပို့လာသူကို ဖုန်းခေါ်ဆိုခြင်း သို့မဟုတ် အီးမေးလ်ပို့ခြင်း အားဖြင့် အတည်ပြုပါ။ သံသယဖြစ်ဖွယ် အီးမေးလ်ကို တိုက်ရိုက် စာမပြန်ပါနှင့်။
- လင့်ခ်တွင် စာလုံးပေါင်းမှားနေခြင်း သို့မဟုတ် ဒိုမိန်းမှားနေခြင်းများကို စစ်ဆေးပါ။ (ဥပမာ၊ လိပ်စာတွင် ".gov" သို့ အဆုံးသတ်ရမည့်အစား ".com" ဖြင့် အဆုံးသတ်ထားခြင်းများ)

- လိပ်စာဘားတန်းတွင် သော့ခတ်ထားသည့် အမှတ်အသားပါရှိခြင်း သို့မဟုတ် browser တွင် “https” ဟူ၍ ပါရှိတိုင်း ဝက်ဘ်ဆိုက် ကို မယုံလိုက်ပါနှင့်။

6. အရေးကြီးသောအချက်အလက်များကို အသုံးမပြုရန် တိုက်တွန်းပါသည်။

သင့်တွင် VPN ရှိလျှင်ပင် ကိုယ်ပိုင်ဘဏ်အကောင့်များ၊ သို့မဟုတ် လူမှုလုံခြုံရေးနံပါတ်များကို စိတ်မချရသည့် လူထုကွန်ရက်များတွင် အသုံးပြုခြင်းကို အားမပေးပါ။ လုံခြုံစိတ်ချရသည့် လူထုကွန်ရက်များတွင်ပင် အန္တရာယ်များလွန်းလှသည်။ ယင်းအကောင့်များကို လူထုဝိုင်ဖိုင်တွင် အသုံးပြုရန်လိုအပ်ပါကကောင်းမွန်စွာချင့်ချိန်ဆုံးဖြတ်ပါ။ ငွေကြေးအထုတ်အသွင်းပြုလုပ်ခြင်းများကို လုပ်ဆောင်ရန်အတွက် သင်၏ စမတ်ဖုန်းမှ hotspot ကို အသုံးပြုခြင်းက ပို၍ကောင်းပါသည်။

7. လုံခြုံစိတ်ချရမှုရှိခြင်း vs. လုံခြုံစိတ်ချရမှုမရှိခြင်း

လူထုဝိုင်ဖိုင်ကွန်ရက်များတွင် အခြေခံအားဖြင့် နှစ်မျိုးနှစ်စားရှိပါသည်-လုံခြုံစိတ်ချရသော ကွန်ရက် နှင့် လုံခြုံစိတ်ချရမှုမရှိသော ကွန်ရက်။

ဖြစ်နိုင်သည့် အခါတိုင်းတွင် လုံခြုံစိတ်ချရသော လူထုကွန်ရက်များနှင့်သာ ချိတ်ဆက်ပါ။ လုံခြုံစိတ်ချရမှုမရှိသော ကွန်ရက်များမှာ လျှို့ဝှက်ကုဒ် သို့မဟုတ် login ကဲ့သို့သော လုံခြုံရေးလုပ်ဆောင်ချက်များမပါရှိပဲ ချိတ်ဆက်နိုင်သည်။ လုံခြုံစိတ်ချရသော ကွန်ရက်သည် ပုံမှန်အားဖြင့် စည်းကမ်းသတ်မှတ်ချက်များကို အသုံးပြုသူမှ သဘောတူပေးရပြီး အကောင့်စာရင်းသွင်းရခြင်း သို့မဟုတ် လျှို့ဝှက်ကုဒ်နံပါတ်ရိုက်ထည့်ရခြင်းများကို ကွန်ရက်နှင့် မချိတ်ဆက်ခင် လုပ်ဆောင်ရပါသည်။

8. သင်၏ firewall ကိုဖွင့်ထားပါ။

လူထုဝိုင်ဖိုင်ကို သင်၏ လက်ပ်တော့ပ်ဖြင့် အသုံးပြုနေသည်ဆိုပါက firewall ကိုဖွင့်ထားပါ။ firewall မှာ သင်၏ကိရိယာကို malware ခြိမ်းခြောက်မှုများမှ အတားအဆီးသဖွယ် ကာကွယ်ထားပေးပါသည်။ ရုတ်တရက်ပေါ်လာရာများ နှင့် အသိပေးကြေညာချက်များကြောင့် အသုံးပြုသူများမှ Windows firewall ကို ပိတ်ထားမိနိုင်ပြီး မေ့လျော့သွားနိုင်ပါသည်။ သင်၏ PC တွင်ပြန်လည်ဖွင့်လိုပါက Control Panel မှတစ်ဆင့် “System and Security” ကိုသွား၍ “Windows Firewall” ကိုရွေးပါ။ အကယ်၍ သင်သည် Mac အသုံးပြုသူဖြစ်ပါက “System Preferences“ သို့သွားပါ၊ ပြီးလျှင် “Security & Privacy” ဆိုဆက်သွားပါ၊ ထိုမှတစ်ဆင့် “Firewall” အကွက်ကိုသွား၍ လုပ်ဆောင်ချက်ကို ဖွင့်ပါ။

9. antivirus ဆော့ဖ်ဝဲ ကို အသုံးပြုပါ။

ထို့ပြင် မိမိ၏လက်ပ်တော့ပ် တွင် တပ်ဆင်ထားသည့် antivirus ပရိုဂရမ်မှာလည်း နောက်ဆုံးပေါ်ဗားရှင်း ဖြစ်စေရန် သေချာစေပါ။ antivirus ပရိုဂရမ်များမှာ လူထုဝိုင်ဖိုင်ကွန်ရက်ကို မျှသုံးနေစဉ်အတွင်း သင်၏စနစ်ကိုmalware များမှဝင်ရောက်ခြင်းကို တားဆီးကာကွယ်ပေးနိုင်ပါသည်။ အကယ်၍ ဗိုင်းရပ်စ်များသင့်ကိရိယာအတွင်းသို့ ဝင်ရောက်နေခြင်း သို့မဟုတ် သံသယဖြစ်ဖွယ်လုပ်ဆောင်ချက်၊တိုက်ခိုက်မှု သို့မဟုတ် malware များ သင့်၏ စနစ်ထဲသို့ ဝင်ရောက်နေခြင်းများ ရှိပါက အချက်ပေးပါလိမ့်မည်။

10. နှစ်ဆင့်ခံထားသော သို့မဟုတ် အဆင့်များစွာခံထားသည့် authentication စနစ်ကိုသုံးပါ။

ဝက်ဘ်ဆိုက်များထဲသို့ မိမိ၏ကိုယ်ရေးအချက်အလက်များဖြင့်ဝင်ရာတွင်အဆင့်များစွာခံထားသည့် authentication စနစ် (MFA) ကို အသုံးပြုပါ။ ယင်းသို့ လုပ်ဆောင်ထားခြင်းအားဖြင့် ဒုတိယ verification ကုဒ်ကို (သင်၏ ဖုန်းသို့ ပို့ပေးခြင်း သို့မဟုတ် app မှတစ်ဆင့် ပို့ပေးခြင်း သို့မဟုတ် ရိုက်ထည့်ရမည့် ကီးပေးပို့ခြင်း) များအားဖြင့် သင့်ကို ကာကွယ်ပေးနိုင်ပါသည်။ ယင်းက ဟတ်ကာအနေဖြင့် သင်၏ အသုံးပြုသူအမည် နှင့် လျှို့ဝှက်ကုဒ်ကို ရရှိသည့်တိုင် သင်၏အကောင့်များကို authentification ကုဒ်မပါပဲ မဝင်ရောက်နိုင်တော့ပါ။

11. သင်၏ ကိုယ်ပိုင်ကိရိယာများကို ခြေရာခံထားပါ။

လူထုနေရာ နှင့် ကားပေါ်များတွင် သင်၏လက်ပ်တော့ပ်၊တက်ပလပ်၊ သို့မဟုတ် စမတ်ဖုန်းများကို လူကွယ်ရာတွင် မထားပါနှင့်။ ဝိုင်ဖိုင်ကွန်ရက်အသုံးပြုရာတွင် ကြိုတင်၍သတိထားသော်လည်း ယင်းက တစ်စုံတစ်ယောက်မှာသင်၏ ပစ္စည်းများ သို့မဟုတ် သင်၏အချက်အလက်များကို ခိုးယူခြင်းမှ တားဆီးနိုင်သည် ဟူသော အဓိပ္ပာယ် မဟုတ်ပါ။ သင်၏ ဝန်းကျင်နှင့် သင့်ပတ်ပတ်လည်တွင် ရှိသောသူများကို သတိထားပါ။

12. အွန်လိုင်းအသုံးပြုရာတွင် ဘေးကင်းလုံခြုံစေရန် တခြားသောအကြံပြုချက်များ။

အထူးသဖြင့် လူထုဝိုင်ဖိုင်ဖြင့် အွန်လိုင်းအသုံးပြုရာတွင် ဘေးကင်းစေရန်အတွက် အကြံပြုချက်များ-

- ခိုင်မာသော လျှို့ဝှက်ကုဒ်များကို သုံးပါ။
- သင်၏ ကိရိယာများကို စကားဝှက်ပုံစံများဖြင့် ပြောင်းလဲထားပါ။
- အီးမေးလ်များ ခိုးယူခံရခြင်းကို သတိထားပါ။

- လူမှုကွန်ယက်တွင် တင်သည့် ပို့စ်များကို သတိထားပါ။ ကိုယ်ရေးအချက်အလက်များစွာကို ဖော်ပြထားခြင်းက ဟတ်ကာများကို မိမိ၏ လျှို့ဝှက်ကုဒ်များကို ခန့်မှန်းရန် ကူညီရာရောက်သည်။
- မိမိမလိုအပ်တော့သည့် အချက်အလက်ဟောင်းများကို ဖျက်ပစ်ပါ။
- ကွန်ရက်မှ သင့်ကို ထပ်ဆင့် ဆော့ဖ်ဝဲလ်များ တပ်ဆင်ခိုင်းခြင်း သို့မဟုတ် browser extension များတပ်ဆင်ခိုင်းလာပါက ချိတ်ဆက်ခြင်းမပြုပါနှင့်။
- သင်၏ ကိရိယာများတွင် နောက်ဆုံးပေါ် update များ နှင့် အချက်အလက်များကို မွမ်းမံတပ်ဆင်ထားခြင်းအားဖြင့် ပြဿနာအတော်များများကို ကာကွယ်နိုင်ပါသည်။