Myanmar Centre for Responsible Business

မူဝါဒရေးရာအနှစ်ချုပ်

ဆိုက်ဘာလုံခြုံရေးနှင့် ဆိုက်ဘာမှုခင်း - မြန်မာနိုင်ငံနှင့် သက်ဆိုင်သည့် အကြောင်းအချက်များ

ဤမူဝါဒရေးရာအနှစ်ချုပ်[1]တွင် ဆိုက်ဘာလုံခြုံရေးနှင့် ဆိုက်ဘာမှုခင်းတို့နှင့် သက်ဆိုင်သည့် ဝေါဟာရများ၊ အယူအဆများ၊ အစဉ်အလာကောင်းများနှင့် ဆိုးကျိုးသက်ရောက်မှု ဖြစ်စေသော အလေ့အထများကို အကျဉ်းချုပ် စုစည်းဖော်ပြထားသည်။ ဆိုက်ဘာလုံခြုံရေးနှင့် ဆိုက်ဘာမှုခင်း ဝေါဟာရများကို တွင်တွင်ကျယ်ကျယ် အသုံးပြုနေကြသော်လည်း ရံဖန်ရံခါတွင် ထိုစကားရပ်များကို ကောင်းမွန်စွာ နားလည်သဘောပေါက်နိုင်ရန် ခက်ခဲတတ်သည်။ သို့ဖြစ်ပါ၍ မြန်မာနိုင်ငံတွင် အဆိုပါ အကြောင်းအရာများကို ဆွေးနွေးသောအခါ သတင်းအချက်အလက် ပိုမိုပြည့်စုံမှု ရှိစေရန် ရည်ရွယ်၍ ဤမူဝါဒရေးရာ အနှစ်ချုပ်အား ထုတ်ဝေခြင်း ဖြစ်ပါသည်။

မြန်မာနိုင်ငံနှင့် ကမ္ဘာတစ်ဝှမ်းလုံးတွင် ကွန်ရက်နှင့် ကိရိယာများကို တိုက်ခိုက်သည့် ဖြစ်ရပ်များမှာ ရေချိန်မြင့်လာသည့် သဘောရှိသည်။ သို့သော်လည်းပဲ လက်ရှိတွင် မြန်မာနိုင်ငံ၌ အဘက်ဘက်မှ ထည့်သွင်းစဉ်းစားထားသော ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ မူဘောင် မရှိသေးသလို ဆိုက်ဘာပြစ်မှု (သို့) အချက်အလက်ကာကွယ်ရေး အတွက် တိတိကျကျ ပြဋ္ဌာန်းထားသော ဥပဒေများလည်း မရှိပေ။

ဤမူဝါဒရေးရာအနှစ်ချုပ်၏ ရည်ရွယ်ချက်မှာ မြန်မာနိုင်ငံအစိုးရ၊ ပုဂ္ဂလိကကဏ္ဍနှင့် အရက်ဖက် လူ့အဖွဲ့အစည်းများကို အားဖြည့်ကူညီ၍ မြန်မာနိုင်ငံ၏ မူဝါဒနှင့် ဥပဒေမူဘောင်ဆိုင်ရာ လစ်ဟာမှုများကို ဖြည့်စည်းပေးနိုင်ရန်နှင့်၊ လုံခြုံရေးနှင့် လူ့အခွင့်အရေးများကို ကာကွယ်ပေးသည့် ဆိုက်ဘာလုံခြုံရေး မူဘောင်(များ) နှင့် ဆိုက်ဘာမှုခင်း ဥပဒေ(များ)ကို ချမှတ်လာနိုင်စေရန်အတွက် ဖြစ်သည်။ ထိုဥပဒေများ ရှိမှသာလျှင် မြန်မာနိုင်ငံ၏ ဒီဂျစ်တယ်စနစ်သည် တိုးတက်ရှင်သန်လာနိုင်မည် ဖြစ်ပြီး ယင်းဥပဒေ လစ်ဟာမှုများကို ဖြည့်ဆည်းရာတွင် လူ့အခွင့်အရေးများကို ကာကွယ်ပေးနိုင်မည့် နည်းလမ်းဖြင့် လုပ်ဆောင်မှသာလျှင် အသုံးပြုသူများ၏ ယုံကြည်မှုကို ရရှိလာမည်ဖြစ်သည်။ လတ်တလော ကမ္ဘာဘဏ်မှ ထုတ်ပြန်ထားသော ဆိုက်ဘာလက်စွဲစာအုပ်တွင် ဖော်ပြထားသည်မှာ -"အင်တာနက်နှင့် အိုင်စီတီပစ္စည်းများကို အသုံးပြုခြင်းမှ ရရှိလာသော "ယုံကြည်မှု" သည် ၎င်းပစ္စည်းများကို အသုံးပြုမှု မြင့်တက်လာစေသည်။ ထို့အပြင်

[1] Privacy International အားကျေးဇူးတင်လိုသည်။ ဤ အနှစ်ချုပ်စာတမ်းသည် Privacy International ၏: After the Gold Rush: Developing Cyber Security Frameworks and Cyber Crime Legislation to Safeguard Privacy and Security (September 2018) ရှိ အချက်များပေါ်တွင် အခြေခံထားပါသည်။

ဆိုက်ဘာလွင်ပြင်၌ အဆိုပါ ယုံကြည်မှု ပတ်ဝန်းကျင်ကို တည်ဆောက်ရာတွင် ပါဝင်သည့် ကဏ္ဍတစ်ရပ်မှာ ကွန်ရက်များ၊ ကိရိယာများနှင့် အချက်အလက်များအား လုံခြုံမှုရှိစေရန် ဆောင်ရွက်ခြင်း နှင့် အခြေခံအခွင့်အရေးများဖြစ်သည့် ပုဂ္ဂလိကလွတ်လပ်ခွင့်နှင့် (အချက်အလက် ကာကွယ်ပေးခြင်း အပါအဝင်) လွတ်လပ်စွာ ထုတ်ဖော်ရေးသားခွင့်တို့အား အသိအမှတ်ပြုပေးခြင်းတို့ကို ညီညီမျှမျှ ဆောင်ရွက်နိုင်ခြင်းပင် ဖြစ်သည်။"[2]

ဆိုက်ဘာလုံခြုံရေးလော (သို့) ဆိုက်ဘာမှုခင်းလော

ဆိုက်ဘာလုံခြုံရေးနှင့် ဆိုက်ဘာမှုခင်းသည် ကွဲပြားခြားနားသောကြောင့် ၎င်းတို့ကို ဖြေရှင်းသောအခါတွင် ဥပဒေတစ်ခုတည်းဖြင့် ပြဿနာအားလုံးကို ဖြေရှင်းရန် အားထုတ်ခြင်းထက် အကြောင်းအရာတစ်ခုချင်းအလိုက် ဦးတည် ရည်ရွယ်ထားသော နည်းလမ်းများကို အသုံးပြု၍ သီးခြားဖြေရှင်းသင့်သည်။

- **ဆိုက်ဘာလုံခြုံရေး** ဆိုသည်မှာ ကွန်ပျူတာစနစ်များကို တိုက်ခိုက်မှုများနှင့် ထိုသို့ တိုက်ခိုက်ခံရခြင်းကြောင့် ဆုံးရှုံးမှုများမှ ကာကွယ်ပေးသည့် နည်းပညာဆိုင်ရာ နည်းလမ်းတစ်ရပ် ဖြစ်သည်။ ကွန်ပျူတာစနစ်များသည် ရှုပ်ထွေးနက်နဲပြီး ယင်းတို့တွင် ထိုစနစ်များ၏ လုံခြုံမှုကို ထိခိုက်စေသည့် အားနည်းချက်များလည်း ပါဝင်နိုင်သည်။ ဆိုက်ဘာလုံခြုံရေး စနစ်ကောင်းများသည် ကွန်ပျူတာစနစ်များတွင် ပါရှိသော အားနည်းချက်များကို ဖော်ထုတ်ပေးနိုင်သလို အဆိုပါ အားနည်းချက်များအား အမျိုးအစား ခွဲခြားသတ်မှတ်ပေးခြင်းနှင့် ပြုပြင်ခြင်းများကိုလည်း ဦးစားပေး ဆောင်ရွက်နိုင်သည်။[3]

- **ဆိုက်ဘာမှုခင်း** ဆိုသည်မှာ ပြစ်မှုကျူးလွန်ရန် ရည်ရွယ်၍ ကွန်ပျူတာစနစ်များအား တရားမဝင် ဝင်ရောက်ကာ ထိုစနစ်များနှင့် ၎င်းတို့တွင် ပါဝင်သော အချက်အလက်များအား ဖျက်ဆီးခြင်း သို့မဟုတ် ပြောင်းလဲခြင်းနှင့် ကွန်ပျူတာစနစ်များကို အသုံးပြု၍ ကျူးလွန်သည့် ပြစ်မှုများအား ဒဏ်ခတ်သည့် ပြစ်မှုဆိုင်ရာ ဥပဒေ နည်းလမ်းတစ်ရပ် ဖြစ်သည်။ ပြစ်မှုဆိုင်ရာဥပဒေအား ဒဏ်ခတ်ရန်နှင့် ဟန့်တားရန် နှစ်မျိုးလုံးအတွက် အသုံးပြုသည်။

ဆိုက်ဘာလုံခြုံရေးကို အများပြည်သူနှင့် ဆိုင်သော ကုန်ပစ္စည်းတစ်ခုကဲ့သို့ ထည့်သွင်း စဉ်းစားသင့်သည်။ အစိုးရ၏ ဆိုက်ဘာလုံခြုံရေးကို ချည်းကပ်လုပ်ဆောင်သော နည်းလမ်းအား ပြည်သူ့ကျန်းမာရေးကို ချည်းကပ်လုပ်ဆောင်သော နည်းလမ်းနှင့် နှိုင်းယှဉ်ကြည့်နိုင်သည်။ အဆိုပါ ပြည်သူ့ကျန်းမာရေးကို ချည်းကပ်လုပ်ဆောင်သော နည်းလမ်းသည် လူတိုင်းအကျိုးရှိစေရန် စုပေါင်း တာဝန်ယူထားခြင်း ဖြစ်သည်။

[2] World Bank and United Nations (2017). Combatting Cybercrime: Tools and Capacity Building for Emerging Economies, Washington, DC., p. 18

[3] ဆိုက်ဘာလုံခြုံရေး နှင့်ပတ်သတ်၍ Privacy International မှ ပိုမိုများပြားသောအရင်းအမြစ်များ https://privacyinternational.org/topics/cyber-security

အစိုးရ၏ အဓိကတာဝန်သည် လျော်ညီသင့်တော်သော ဆိုက်ဘာလုံခြုံရေး မူဘောင်တစ်ရပ်ကို ရေးဆွဲချမှတ်ရန်နှင့် ၎င်းအား အကောင်အထည်ဖော် ဆောင်ရွက်ခြင်းကို သေချာစေရန် ဖြစ်သည်။

ဆိုက်ဘာလုံခြုံရေး ဆောင်ရွက်ရာတွင် ဆိုက်ဘာတိုက်ခိုက်မှုအားလုံးကို ကာကွယ်ရန် မဖြစ်နိုင်ကြောင်းကိုတော့ သတိပြုရပေမည်။ စနစ်များမှာ မူလကတည်းက အားနည်းသည့်အပြင် ထိုစနစ်များသည် အချိန်ကာလတစ်ခုတွင်တော့ တိုက်ခိုက်မှုများကို အနည်းနှင့်အများ ကြုံတွေ့ရလိမ့်မည် ဖြစ်သည်။ တိုက်ခိုက်မှုများကို တတ်နိုင်သရွေ့ ကာကွယ်ခြင်းမှာ အရေးကြီးသည် မှန်သော်လည်း၊ ကောင်းမွန်သော ဆိုက်ဘာလုံခြုံရေးတွင် တွန်းလှန်လွန်မြောက်နိုင်စွမ်းရှိခြင်း(Resilience)သည်လည်း သာတူညီမျှ အရေးကြီးပါသည်။ တွန်းလှန်လွန်မြောက်နိုင်စွမ်းရှိခြင်းဆိုသည်မှာ ကွန်ပျူတာစနစ်တွင် တိုက်ခိုက်မှု ခံရသည့်အခါ၌ အချက်အလက် ဆုံးရှုံးမှုများနှင့် အဆုံးစွန် ပျက်စီးဆုံးရှုံးမှုများ ဖြစ်ပေါ်စေခြင်းမရှိပဲ ကောင်းစွာ ပြန်လည် ထူထောင်နိုင်ခြင်းပင် ဖြစ်သည်။

ဆိုက်ဘာလုံခြုံရေး မြှင့်တင်နိုင်ရန် လုပ်ဆောင်ရမည့်အချက် (၆) ချက်

၁။ <u>ဥပဒေတစ်ခုတည်း သီးသန့် ပေါ်ပေါက်လာရေးထက် ဆိုက်ဘာလုံခြုံရေး မူဘောင်တစ်ရပ် (Cyber Security Framework) ကို ဦးတည်၍အကောင်အထည်ဖော်ဆောင်ရွက်ရန်။</u>

ဆိုက်ဘာလုံခြုံရေးဟု ဆိုရာတွင် ကွဲပြားသော်လည်း အချင်းချင်း ကူညီထောက်ပံ့ပေးထားသည့် ရှေ့ပြေးလုပ်ဆောင်ချက်များနှင့် နည်းလမ်းများ ပါဝင်သည်။ ဥပဒေပြဋ္ဌာန်းခြင်းသည် ထိုအချက်များတွင် ပါဝင်သည့် အစိတ်အပိုင်းတစ်ခုသာ ဖြစ်သည်။ ဥပဒေရေးရာနှင့် သက်ဆိုင်ခြင်း မရှိသော အခြားအချက်များတွင် လုံခြုံရေးဆိုင်ရာ အနိမ့်ဆုံး စံနှုန်းသတ်မှတ်ချက်များ၊ လုံခြုံရေးဆိုင်ရာ သုတေသန ပြုလုပ်ရန်အတွက် ရင်းနှီးမြှုပ်နှံမှု၊ အများပြည်သူဆိုင်ရာ အဖွဲ့အစည်းများနှင့် အဓိကစက်မှုလုပ်ငန်းများ၏ လုံခြုံရေးဆိုင်ရာ စာရင်းစစ်ဆေးခြင်း စသည်တို့ ပါဝင်သည်။ ရှင်းလင်းပြီး တစ်သမတ်တည်းဖြစ်သော မူဘောင်များ၊ ဗျူဟာများနှင့် မူဝါဒများ (ဥပမာ - အမျိုးသား ဆိုက်ဘာလုံခြုံရေးဗျူဟာ)သည် လုံခြုံရေးစံနှုန်းများကို သတ်မှတ်ပေးသလို လူ့အခွင့်အရေးများကိုလည်း အကာအကွယ်ပေးပါသည်။

၂။ <u>လူပုဂ္ဂိုလ်များ၊ ကိရိယာများနှင့် ကွန်ရက်များအား ကာကွယ်ခြင်းကို ဆိုက်ဘာလုံခြုံရေး ဗျူဟာ/ မူဝါဒတိုင်း၏ ပင်မရည်ရွယ်ချက်အဖြစ် ဦးစားပေးလုပ်ဆောင်ရန်။</u>

ကောင်းမွန်သော ဆိုက်ဘာလုံခြုံရေး မူဝါဒများနှင့် အလေ့အကျင့်များသည် လူပုဂ္ဂိုလ်များနှင့် ၎င်းတို့၏ လူ့အခွင့်အရေးများကို အဓိက ဦးတည်ထားပြီး လူ့အခွင့်အရေးများကို ပို၍ ခိုင်မာလာစေရန်နှင့် ကာကွယ်ပေးနိုင်ရန် တို့ကိုသာ ဗျူဟာ၏ ပင်မရည်ရွယ်ချက် အဖြစ် သတ်မှတ်၍ ဆောင်ရွက်သည်။

• **<u>လူပုဂ္ဂိုလ်များအား</u> ကာကွယ်ခြင်း** - ဆိုက်ဘာလုံခြုံရေးမူဘောင်များတွင် ကုမ္ပဏီများနှင့် အများပြည်သူဆိုင်ရာ အဖွဲ့အစည်းများက ရယူထားသော ကိုယ်ရေးကိုယ်တာ အချက်အလက်များအား အမြတ်ထုတ် အသုံးချခြင်းမှ ကာကွယ်ပေးသည့် အချက်အလက် ကာကွယ်ရေး ဥပဒေများ ပါဝင်ရမည်။

• **<u>ကိရိယာများအား</u> ကာကွယ်ခြင်း** - "အင်တာနက်ဆိုင်ရာ ကိရိယာများ" (Internet of Things) ဟု အသိများသည့် အင်တာနက်ချိတ်ဆက်ကိရိယာများ ဖြစ်သော ဝိုင်ဖိုင်လွှင့်ပေးသည့်စက်များ (routers)၊ ကွန်ရက်ချိတ်ဆက်ကင်မရာများ (webcams) နှင့် အခြားသော အိမ်သုံးပစ္စည်းများကို လုံခြုံမှုရှိစေခြင်းသည် ဆိုက်ဘာလုံခြုံရေး၏ အဓိက ရည်ရွယ်ချက် ဖြစ်သင့်သည်။ ၎င်းကိရိယာများသည် ကာကွယ်သင့်သော ပုဂ္ဂိုလ်ရေးရာ အချက်အလက်များအား ထုတ်လုပ်ခြင်း၊ စုဆောင်းခြင်းနှင့် တစ်ဆင့် ထုတ်လွှင့်ခြင်းတို့ကို ပြုလုပ်နိုင်သဖြင့် ပုဂ္ဂလိကလွတ်လပ်ခွင့်ဆိုင်ရာ အန္တရာယ်များ ကျရောက်လာနိုင်သည်။ ထို့ပြင် ကွန်ရက်နှင့် ချိတ်ဆက်ထားရာမှတစ်ဆင့် လုံခြုံရေးဆိုင်ရာ အန္တရာယ်များလည်း ဖြစ်ပေါ်စေနိုင်သောကြောင့် ယင်းကိရိယာများသည် ကွန်ရက်လုံခြုံရေးဆိုင်ရာ ကာကွယ်မှုတွင် အားအနည်းဆုံးချိတ်ဆက်မှု ဖြစ်နေတတ်သည်။

• **<u>ကွန်ရက်များအား</u> ကာကွယ်ခြင်း** - ကောင်းမွန်သော ကွန်ရက်လုံခြုံရေး ဆိုသည်မှာ တိုက်ခိုက်မှု ဖြစ်ပွားခြင်းများကို နည်းပါးစေပြီး ကွန်ရက်ပေါ်တွင် စစ်မှန်သော ကိရိယာများမှတစ်ဆင့် အမှန်တကယ် သက်ဆိုင်သော လူပုဂ္ဂိုလ်များအား မှန်ကန်သည့် ဝန်ဆောင်မှုစစ်စစ်များကိုသာ သုံးစွဲရယူရန် ခွင့်ပြုပြီး ထိုသို့မဟုတ်သော အခြားသူများနှင့် အခြားအရာအားလုံးကို တားဆီးပိတ်ပင်ထားနိုင်ခြင်းပင် ဖြစ်သည်။

၃။ <u>အဘက်ဘက်မှ စဉ်းစားထားသော အချက်အလက်ကာကွယ်ရေးဥပဒေတစ်ရပ် (data protection law) ကို ပြဋ္ဌာန်းကျင့်သုံးအကောင်အထည်ဖော်ဆောင်ရွက်ရန်။</u>

ကိုယ်ရေးကိုယ်တာ အချက်အလက်များအား ကုမ္ပဏီများနှင့် ပြည်သူ့ဆိုင်ရာ အဖွဲ့အစည်းများက အမြတ်ထုတ် အသုံးချခြင်း၊ ပြည်သူများ၏ အချက်အလက်များအား အလွန်အကျွံ ကောက်ယူခြင်း၊ လုံခြုံရေး အားနည်းခြင်းနှင့် ထိုသို့ အားနည်းခြင်းကြောင့် နောက်ဆုံးတွင် ယင်းအချက်အလက်များ ခိုးယူခံရနိုင်ခြင်း အစရှိသည့် အခြေအနေများမှ ကာကွယ်ပေးနိုင်မည့် ဥပဒေဆိုင်ရာ သတ်မှတ်ချက်များ ပြဋ္ဌာန်းပေးရမည်။ မြန်မာနိုင်ငံတွင် ယခုအချိန်ထိ အချက်အလက်ကာကွယ်ရေးဆိုင်ရာ ဥပဒေတစ်ရပ် မရှိသေးပေ။[4]

[4] မြန်မာ့စီးပွားရေးကဏ္ဍတာဝန်ယူမှုရှိရေး အထောက်အကူပြုဌာန၏ လုံခြုံရေးနှင့်အချက်အလက် ကာကွယ်ရေးနှင့်ပတ်သတ်သော တွဲဖက်မူဝါဒရေးရာအကျဉ်းချုပ်တွင် ကြည့်ပါ။

၄။ အရေးကြီးသော အခြေခံ အဆောက်အအုံများ (Critical Infrastructure) ကို ခွဲခြားသတ်မှတ်ပြီး ဦးစားပေးဆောင်ရွက်ရန်။

အရေးကြီးသော အခြေခံ အဆောက်အအုံ ဆိုသည်မှာ အခြေခံ လိုအပ်သော စနစ်များ ဖြစ်ပြီး ၎င်းစနစ်များရှိ ထိခိုက်မှု သို့မဟုတ် ဆုံးရှုံးမှုများသည် နိုင်ငံ၏ လုပ်ငန်းစဉ်များနှင့် ပြည်သူများ၏ လုံခြုံရေး စသည့် ကိစ္စရပ်များအပေါ်တွင် သိသာထင်ရှားသော သက်ရောက်မှုများ ဖြစ်ပေါ်စေနိုင်သည်။ အစိုးရတိုင်းသည် မည်သည့် အခြေခံအဆောက်အအုံက အရေးကြီးကြောင်းကို ဆုံးဖြတ်ရမည် ဖြစ်သော်လည်း အများအားဖြင့် ရွေးချယ်သတ်မှတ်ထားသော အခြေခံ အဆောက်အအုံများတွင် စွမ်းအင်ကဏ္ဍ (လျှပ်စစ်မီး၊ စက်သုံးဆီ၊ ဓာတ်ငွေ့)၊ သယ်ယူပို့ဆောင်ရေးကဏ္ဍ (လေကြောင်း၊ မီးရထား၊ ရေကြောင်း၊ ကားလမ်း)၊ ဘဏ္ဍာရေးနှင့် ငွေကြေး စျေးကွက်ဆိုင်ရာ အခြေခံ အဆောက်အအုံများ၊ ဒီဂျစ်တယ် အဆောက်အအုံ၊ ဓာတုပစ္စည်းများ၊ အစားအသောက်၊ ကျန်းမာရေးကဏ္ဍ၊ ရေနှင့် အရေးပေါ်ဝန်ဆောင်မှုများ စသည်တို့ ပါဝင်သည်။

၅။ လုံခြုံရေးဆိုင်ရာ ဖြစ်ရပ်များအတွက် တုံ့ပြန်နိုင်သည့် အဖွဲ့များ ဖွဲ့စည်းထူထောင်ရန်။

ဤကျွမ်းကျင်ပညာရှင်အဖွဲ့များသည် လုံခြုံရေးဆိုင်ရာ ဖြစ်ရပ်တစ်ခု ပေါ်ပေါက်လာလျှင် ရှေ့တန်းက တုံ့ပြန်ဆောင်ရွက်ပေးသည်။ ၎င်းတို့သည် ဆိုက်ဘာတိုက်ခိုက်မှုများကို ဖြစ်ပေါ်စေသော ကိရိယာများနှင့် ဝန်ဆောင်မှုများအား အဓိကကိုင်တွယ်ဖြေရှင်းပေးသည်။ ထိုအဖွဲ့များသည် အထူးသဖြင့် အစိုးရဌာန ဆိုင်ရာများနှင့် မသက်ဆိုင်သည့် သီးခြားအဖွဲ့များသာ ဖြစ်သင့်ပေသည်။ အများအားဖြင့် တွေ့ရတတ်သည်မှာ အိုင်စီတီ အဆောက်အအုံများနှင့် သက်ဆိုင်သည့် လုံခြုံရေးဆိုင်ရာ ကိစ္စရပ်များကို ကိုင်တွယ်သော ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ ဖြစ်ရပ်များအတွက် တုံ့ပြန်နိုင်သည့် အဖွဲ့ (Cyber Security Incident Response Team – CSIRT) ဖြစ်သည်။[5] မြန်မာနိုင်ငံတွင်လည်း ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ ဖြစ်ရပ်များကို ဖြေရှင်းပေးပြီး အကျိုးအမြတ်မယူသော အဖွဲ့အစည်းတစ်ခုဖြစ်သည့် မြန်မာနိုင်ငံကွန်ပျူတာ အရေးပေါ်တုံ့ပြန်ရေးအဖွဲ့ Myanmar Computer Emergency Response Team (mmCERT) ရှိပါသည်။[6]

[5] ပထမဦးစွာ ထိခိုက်မှုများကို တုံ့ပြန်ခြင်းနှင့်လုံခြုံရေးအဖွဲ့အစည်းများ၏ ကမ္ဘာ့ဖိုရမ်၊ သင်တန်းနှင့်အလုပ်ရုံဆွေးနွေးပွဲများ လုပ်ဆောင်မှုနှင့် ပို၍များပြားသော အရင်းအမြစ်များကို how to set up a CSIRTတွင် ရနိုင်ပါသည်။ https://www.first.org/ နှင့် how to set up a CSIRT ကိုကြည့်ပါ။ www.first.org/education/trainings

[6] https://www.mmcert.org.mm/

၆။ <u>ဆိုက်ဘာခြိမ်းခြောက်မှု အန္တရာယ်ဆိုင်ရာ လေ့လာဆန်းစစ်မှုအား စနစ်တကျ လုပ်ဆောင်ရန်နှင့် ပြန်လည် ထူထောင်ရေး အစီအစဉ်များကို အကောင်အထည်ဖော်ဆောင်ရွက်ရန်။</u>

ဆိုက်ဘာခြိမ်းခြောက်မှု အန္တရာယ်ဆိုင်ရာ လေ့လာဆန်းစစ်မှုတွင် နိုင်ငံတစ်နိုင်ငံ၏ ဆိုက်ဘာရေးရာ တိုက်ခိုက်မှုများကို ခုခံနိုင်စွမ်း အားနည်းနေသည့် ဖြစ်နိုင်ချေ အကြောင်းရင်းများ (ဥပမာ - ခေတ်နှင့် မလျော်ညီတော့သော အခြေခံအဆောက်အအုံများ) ကို ပါဝင်သုံးသပ်ထားသည်။ ထိုခြိမ်းခြောက်မှုများကို လေ့လာဆန်းစစ်ခြင်းသည် အကြီးမားဆုံး အန္တရာယ်များကို ဖြေရှင်းပေးနိုင်မည့် ကန့်သတ်အရင်းအမြစ်များအား ခွဲဝေသတ်မှတ်ရာတွင် အထောက်အကူပြုသည်။ ယခု ဆန်းစစ်မှုများကို ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ ဖြစ်ရပ်များအတွက် တုံ့ပြန်နိုင်သည့် အဖွဲ့များက (CSIRTS) ကူညီဆောင်ရွက်ပေးနိုင်ပါသည်။

ဆိုက်ဘာလုံခြုံရေးကျဆင်းမှုကို ရှောင်ရှားနိုင်မည့် အချက် (၂) ချက်

အချို့သော လုပ်ဆောင်ချက်များသည် ဆိုက်ဘာလုံခြုံရေးကို ပိုမို မြှင့်တင်နိုင်ခြင်း မရှိပဲ ပိုမိုကျဆင်းခြင်းကိုသာ ဖြစ်ပေါ်စေပါသည်။

၁။ <u>တိုက်ခိုက်သည့် စနစ်များအပေါ်တွင် အချိန်နှင့် အရင်းအမြစ်များ မဖြုန်းတီးမိစေရန်။</u>

မိုဘိုင်းဘဏ်စနစ်မှစ၍ အီလက်ထရောနစ်ကုန်သွယ်ရေးအဆုံး နေ့စဉ်လုပ်ငန်းဆောင်တာများမှာ တစ်ဖြည်းဖြည်း အွန်လိုင်းစနစ်သို့ ပြောင်းလဲလာခြင်းကြောင့် နိုင်ငံတွင်း စီးပွားရေးနှင့် အမျိုးသားလုံခြုံရေး ဆိုင်ရာ ကိစ္စရပ်များတွင် ဆိုက်ဘာမှုခင်း အန္တရာယ်များ ပိုမိုမြင့်တက်လာနိုင်သည်။ ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ ပြဿနာများကို ဖြေရှင်းရန်အတွက် မြန်မာနိုင်ငံရှိ အရင်းအမြစ်များနှင့် ကျွမ်းကျင်မှုများမှာ အကန့်အသတ်နှင့်သာ တည်ရှိနေပေသည်။ စီးပွားရေးနှင့် အစိုးရ ဝန်ဆောင်မှု ကိစ္စရပ်များတွင် ယုံကြည်မှုတံတား တည်ဆောက်နိုင်ရန် ရည်ရွယ်၍ မြန်မာနိုင်ငံရှိ အရင်းအမြစ်များကို ခြိမ်းခြောက်မှု အန္တရာယ်များကို ဖော်ထုတ်၍ ခုခံမှုပြုပေးနိုင်မည့် စနစ်များတွင်သာ ရင်းနှီးမြှုပ်နှံသင့်သည်။ ထိုသို့မဟုတ်ပဲ ခုခံမှုပြုပေးနိုင်မည့် စနစ်များအစား တိုက်ခိုက်သည့် စနစ်များဖြစ်သည့် စောင့်ကြည့်လေ့လာခြင်းနှင့် စောင့်ကြပ်ကြည့်ရှုခြင်းဆိုင်ရာ ပစ္စည်းများတွင် ကန့်သတ် အရင်းအမြစ်များအား ရင်းနှီးမြှုပ်နှံလိုက်ခြင်းသည် လူပုဂ္ဂိုလ်များ၊ ကိရိယာများနှင့် ကွန်ရက်များ၏ ဆိုက်ဘာလုံခြုံရေးစနစ်များအပေါ်တွင် အန္တရာယ်သက်ရောက်မှုများ ကျရောက်လာနိုင်သည်။

၂။ <u>ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ လုပ်ငန်းစဉ် ကိစ္စရပ်များကို လျှို့ဝှက် ဆောင်ရွက်ခြင်း မပြုရန်။</u>

အများပြည်သူ ပါဝင်သည့် ညှိနှိုင်းဆွေးနွေးတိုင်ပင်မှုများမှ တစ်ဆင့် ရှင်းလင်းပြည့်စုံ၍ အလွယ်တကူ လက်လှမ်းမီသော ဆိုက်ဘာ လုံခြုံရေး မူဝါဒနှင့် ဥပဒေရေးရာ မူဘောင်များကို အကောင်အထည်ဖော် ဆောင်ရွက်သင့်သည်။ နိုင်ငံ၏ လုပ်ထုံးနည်းလမ်းနှင့် ၎င်းအား အကောင်အထည်ဖော်ခြင်းဆိုင်ရာ ကိစ္စရပ်များကို

လျှို့ဝှက်ထားလျှင် ပြည်သူလူထုနှင့် စီးပွားရေးလုပ်ငန်းများသည် ခြိမ်းခြောက်မှုများနှင့် ပတ်သက်၍ ဗဟုသုတမရှိခြင်း၊ မိမိကိုယ်မိမိ မည်သို့ ကာကွယ်ရမည်ကို မသိခြင်း စသည့် ဆိုးကျိုးများ သက်ရောက်နိုင်ပါသည်။ ထိုသို့ လျှို့ဝှက်ဆောင်ရွက်ခြင်းသည် ဆိုက်ဘာလုံခြုံရေးကို သွေဖယ်စေမည့် ဆန့်ကျင်ဘက်နည်းလမ်း တစ်ရပ်ပင် ဖြစ်သည်။

ဆိုက်ဘာမှုခင်းအား မည်သို့ ဖြေရှင်းဆောင်ရွက်သင့်သနည်း။

ဆိုက်ဘာလုံခြုံရေးသည် ကွန်ပျူတာစနစ်များအား နည်းပညာဖြင့် လုံခြုံမှုရှိစေရန် ဆောင်ရွက်ခြင်းနှင့် သက်ဆိုင်သော်လည်း ဆိုက်ဘာမှုခင်းမှာမူ ကွန်ပျူတာ အသုံးပြု၍ ကျူးလွန်ထားသော ပြစ်မှုများကို ဟန့်တားခြင်းနှင့် အပြစ်ပေးခြင်းတို့ကို လုပ်ဆောင်သည်။ ဆိုက်ဘာမှုခင်းတွင် နယ်စပ်မရှိသဖြင့် ထိရောက်သည့် အရေးယူဆောင်ရွက်မှု ဖြစ်လာစေရန်အတွက် နယ်စပ်ဖြတ်ကျော် ပူပေါင်းပါဝင်မှုများ ဆောင်ရွက်ရန် ရုံဖန်ရုံခါ လိုအပ်လေ့ရှိသည်။ နယ်စပ်ဖြတ်ကျော် ပူပေါင်းပါဝင်မှု၏ လိုအပ်ချက်မှာ လုပ်ရပ်တစ်ရပ်သည် ရာဇဝတ်မှုမြောက်သည်ဟူ၍ အစိုးရနှစ်ဘက်လုံးက သဘောတူညီရန် လိုအပ်သောကြောင့် အတိအကျ အဓိပ္ပါယ် ဖွင့်ဆိုထားသော ပြစ်မှုအမျိုးအစားစာရင်းမှာ အသုံးဝင်သည်။ ဆိုက်ဘာမှုခင်းနှင့် ပတ်သက်၍ တစ်ကမ္ဘာလုံး အတိုင်းအတာဖြင့် လက်ခံထားသော သတ်မှတ်ချက် မရှိသော်လည်း ၎င်းတို့တွင် ယေဘုယျအားဖြင့် မတူညီသော ပြစ်မှုအုပ်စု နှစ်စု ပါဝင်သောကြောင့် ၎င်းတို့ကို ကွဲကွဲပြားပြား၊ ထင်ထင်ရှားရှား ဖြစ်စေရန်အတွက် မူဝါဒများနှင့် ဥပဒေများ ပြဋ္ဌာန်းသတ်မှတ်ပြီး ဆောင်ရွက်သင့်သည်။

ကွန်ပျူတာစနစ်များကို ဦးတည်တိုက်ခိုက်သည့် ဆိုက်ဘာမှုခင်းများ (Cyber Dependent Crimes) –

ဤပြစ်မှုများကို ကျူးလွန်လျှင် ရာဇဝတ်မှုမြောက်ပြီး ယင်းတို့သည် ကွန်ပျူတာ သို့မဟုတ် ကိရိယာ တစ်ခုခုကို အသုံးပြု၍သာ ကျူးလွန်နိုင်သော ပြစ်မှုများဖြစ်သည်။ ၎င်းတို့သည် ကွန်ပျူတာစနစ်နှင့် ကွန်ရက်များ၊ ၎င်းတို့အတွင်း သိမ်းဆည်းသိုလှောင်၍ ပြင်ဆင်ထားသည့် အချက်အလက်များ၏ လျှို့ဝှက်ထားသည့် အခြေအနေ၊ မူလပကတိအတိုင်း ရှိနေခြင်း၊ ရယူသုံးစွဲနိုင်ခြင်းတို့အား ဦးတည်ပြီး တိုက်ခိုက် ကျူးလွန်သော ပြစ်မှုဆိုင်ရာ လုပ်ရပ်များ ဖြစ်သည်။ အဓိကကျသော အခြေခံမူမှာ ပြစ်မှုကျူးလွန်ရန် ရည်ရွယ်ချက်ဖြင့် ကွန်ပျူတာစနစ်များအား တရားမဝင် ဝင်ရောက်မှုကို အပြစ်ပေးရန် ဖြစ်သည်။ ဥပမာများမှာ -

- ကွန်ပျူတာစနစ်များ ထိခိုက်သွားစေရန် သို့မဟုတ် ရပ်တန့်သွားစေရန် ရည်ရွယ်၍ ၎င်းတို့အတွင်းသို့ ခွင့်ပြုချက် မရှိပဲ ဝင်ရောက်ခြင်း၊
- လိမ်လည်ပြီး အချက်အလက်များ ခိုးယူခြင်း (ဘဏ်ကဲ့သို့ ဟန်ဆောင်၍ အခြားလူများ၏ လျှို့ဝှက် စကားဝှက်များနှင့် ကိုယ်ရေးအချက်အလက်များ ရယူနိုင်ရန်အတွက် အီးမေးလ်အတုများ ပို့ခြင်း)၊
- ဗိုင်းရပ်စ် (viruses) နှင့် ထရိုဂျန် (trojans) များ ဖြန့်ဝေခြင်း၊

- ဝက်(ဘ်)ဆိုက်များကို ရုပ်တန့်သွားစေသည့် Distributed Denial of Service (DDOS) တိုက်ခိုက်မှုအား လုပ်ဆောင်ခြင်း၊
- ကီးဘုတ်ပေါ်တွင် နှိပ်လိုက်သော လက်ကွက်များကို မှတ်ထားခြင်း၊ လျှို့ဝှက် စကားဝှက်များကို ခိုးယူခြင်း စသည်တို့ကို ပြုလုပ်နိုင်သော မဲလ်ဝဲများအား ဖြန့်ဝေခြင်း စသည်တို့ ပါဝင်သည်။

ဆိုက်ဘာနည်းလမ်းများကို အသုံးပြု၍ ကျူးလွန်သော မှုခင်းများ (Cyber enabled crimes)_- ယင်းတွင် ပိုမိုကျယ်ပြန့်သည့် တည်ရှိပြီးဖြစ်သော ပြစ်မှုများကို နည်းပညာ အသုံးပြု၍ နည်းလမ်းအသစ်ဖြင့် ကျူးလွန်သော မှုခင်းများ ပါဝင်ပြီး ၎င်းတို့ကို အွန်လိုင်း အသုံးပြု၍ ဖြစ်စေ၊ အသုံးမပြုပဲ ဖြစ်စေ ကျူးလွန်နိုင်သည်။ ဥပမာများ အနေနှင့် -

- အီးမေးလ်ပို့၍ ကျူးလွန်သော လိမ်လည်မှုများ၊
- ကလေးသူငယ်များကို ညှင်းပန်းနှိပ်စက်ခြင်း (သို့) စော်ကားခြင်းဆိုင်ရာ ဓာတ်ပုံများအား ဖြန့်ဝေမှု၊
- "ကလဲ့စားချေရန်ရည်ရွယ်ထားသော ညစ်ညမ်းခွေများ" ဟု အသိများသော ရင်းနှီးမှုလွန်ကဲသည့် ပုံများကို ခွင့်ပြုချက်မရှိပဲ ဖြန့်ဝေမှု စသည်တို့ ပါဝင်သည်။

အချို့အစိုးရများသည် ပြစ်မှုလည်း မမြောက်သော၊ ပြစ်မှုမြောက်သည်ဟုလည်း မသတ်မှတ်သင့်သော လုပ်ရပ်များအား အင်တာနက်ပေါ်၌ လုပ်ဆောင်ခြင်း သက်သက်ပေါ် အခြေခံ၍ ဆိုက်ဘာမှုခင်းဟု သတ်မှတ်လေ့ရှိသဖြင့် ၎င်းကိစ္စရပ်အပေါ်တွင် စိုးရိမ်မှုများ ဖြစ်ပေါ်လာကြသည်။ ထိုသို့သတ်မှတ်ရာတွင် ပြစ်မှုကျူးလွန်လိုသည့် ရည်ရွယ်ချက် ရှိခြင်း၊ မရှိခြင်း အပေါ်တွင် ထပ်ဆောင်းလိုအပ်ချက်များ မလိုအပ်စေဘဲ စာလုံးရေ ဖောင်းပွ၍ တိကျမှုမရှိသော လုပ်ရပ်များ (ဥပမာ - "နိုင်ငံတော်၏ ဂုဏ်သရေကို ငြိုးနွမ်းစေသော သတင်းအချက်အလက်များကို ဖြန့်ဝေခြင်း"၊ "ယဉ်ကျေးမှုတန်ဖိုးများကို စော်ကားခြင်း"၊ "အီးမေးလ် မြောက်မြားစွာအား မကြာခဏပို့ခြင်း") ကို ဥပဒေတွင် ပြဋ္ဌာန်းထားခြင်းများ ပါဝင်သည်။ ထိုသို့ ဝေဝါးသော ပြဋ္ဌာန်းချက်များသည် နိုင်ငံရေး ပြိုင်ဘက်များနှင့် အစိုးရအား ဝေဖန်ထောက်ပြခြင်းတို့ကို အရေးယူရန်၊ အဂတိလိုက်စားမှုကို စုံစမ်းစစ်ဆေးနေသော သတင်းထောက်များအား ဖမ်းဆီးအကျဉ်းချရန်၊ လွတ်လပ်စွာ ထုတ်ဖော်ပြောဆိုခွင့်အား ပိတ်ပင်တားမြစ်ရန်နှင့် အကျယ်အားဖြင့် အင်တာနက်အသုံးပြုမှုကို ဟန့်တားရန် စသော ကိစ္စရပ်များတွင် လွဲမှားစွာ အသုံးပြုမှုများ ဖြစ်ပေါ်စေနိုင်သဖြင့် အပြည်ပြည်ဆိုင်ရာ လူ့အခွင့်အရေးဥပဒေကို ချိုးဖောက်နိုင်ချေရှိသည်။

ကောင်းမွန်သော ဆိုက်ဘာမှုခင်းဥပဒေများ ပေါ်ထွန်းလာရန် လုပ်ဆောင်ရမည့် အဆင့် (၃) ဆင့်

၁။ <u>ဆိုက်ဘာမှုခင်းဥပဒေပြဋ္ဌာန်းရာတွင် လူ့အခွင့်အရေး အကာအကွယ်ပေးခြင်းများနှင့် ကိုက်ညီမှုရှိစေရေး အတွက် ဆောင်ရွက်ရန်။</u>

ဆိုက်ဘာမှုခင်းဥပဒေများကို မြန်မာနိုင်ငံအနေဖြင့် လိုက်နာရမည့် လူ့အခွင့်အရေး ကာကွယ်ခြင်းဆိုင်ရာ အပြည်ပြည်ဆိုင်ရာ ကတိကဝတ်များနှင့် ကိုက်ညီအောင် ရေးဆွဲသင့်သည်။ မိမိပိုင်နက်ကို ကျော်လွန်၍ သိမ်းဆည်းထားသော အချက်အလက်များအား မည်သို့သော နည်းလမ်းမျိုးဖြင့် ရယူသုံးစွဲသည်ဖြစ်စေ ပြစ်မှုဆိုင်ရာ ကိစ္စရပ်များအတွက် အီလက်ထရောနစ် သက်သေများအား ရယူခြင်းအား ထည့်သွင်း ပြဋ္ဌာန်းသင့်သည်။ ထိုသို့ လုပ်ဆောင်သည့်အခါ၌ တရားဥပဒေနှင့် ညီညွတ်ခြင်း၊ အမှန်တကယ် လိုအပ်မှုရှိခြင်း၊ အချိုးအစားညီမျှမှုရှိခြင်း၊ တရားရုံး၏ တရားဝင်ခွင့်ပြုမိန့် ကြိုတင်ရရှိထားခြင်း၊ ထိရောက်သော ကြီးကြပ်မှုရှိခြင်း၊ ကြိုတင်အကြောင်းကြားစာ ပေးပို့ထားခြင်း၊ ထိရောက်သော ကုစားခွင့် ရရှိခံစားရခြင်းတို့ကို အခြေခံထားသည့် လူ့အခွင့်အရေး အခြေခံမူများနှင့် အကာအကွယ်ပေးမှုများ ပါဝင်သင့်ပါသည်။[7]

၂။ <u>ကွန်ပျူတာစနစ်များကို ဦးတည်တိုက်ခိုက်သည့် ဆိုက်ဘာမှုခင်းများ (Cyber Dependent Crimes) အား တိတိကျကျ အဓိပ္ပာယ် သတ်မှတ်ရန်။</u>

ကွန်ပျူတာစနစ်နှင့် ကွန်ရက်များ၊ ၎င်းတို့အတွင်း သိမ်းဆည်းသိုလှောင်၍ ပြင်ဆင်ထားသည့် အချက်အလက်များ၏ လျှို့ဝှက်ထားသည့် အခြေအနေ၊ ပုံမပျက် ရှိနေခြင်း၊ ရယူသုံးစွဲနိုင်ခြင်း စသည်တို့ကို ပြစ်မှတ်ထား ကျူးလွန်ရန် ရည်ရွယ်၍ တရားမဝင် အသုံးပြုခြင်းကို ဒဏ်ခတ်နိုင်ရန်အတွက် ဤပြစ်မှုများကို အဓိပ္ပါယ်ဖော် နားလည်သင့်သည်။

၃။ ဆိုက်ဘာနည်းလမ်းများကို အသုံးပြု၍ ကျူးလွန်သော မှုခင်းများ (Cyber enabled crimes) <u>နှင့်ပတ်သက်၍ ဘက်စုံပြည့်စုံသော ဥပဒေရေးရာ မူဘောင်များကို လုပ်ဆောင်ရာတွင် ICT အသုံးပြုမှုတင်မကပဲ ပြစ်မှု၏ အခြေခံ သဘောသဘာဝကိုပါ အလေးပေးစဉ်းစားခြင်း ။</u>

ဆိုက်ဘာနည်းလမ်းများကို အသုံးပြု၍ ကျူးလွန်သော မှုခင်းများ (Cyber enabled crimes) များသည် လိမ်လည်မှု သို့မဟုတ် ကလေးသူငယ် ညှင်းပန်းနှိပ်စက်မှုဆိုင်ရာ ဓာတ်ပုံများအား ဖြန့်ဝေမှု စသည့် တည်ရှိပြီးဖြစ်သော ပြစ်မှုများကို နည်းပညာ အသုံးပြု၍ နည်းလမ်းအသစ်ဖြင့် ကျူးလွန်သော မှုခင်းများ ပါဝင်ပြီး ၎င်းတို့ကို အွန်လိုင်း အသုံးပြု၍ ဖြစ်စေ၊ အသုံးမပြုပဲ ဖြစ်စေ ကျူးလွန်နိုင်သည်။ ထို့ကြောင့် ဘက်စုံရှုထောင့်မှ ထည့်သွင်းစဉ်းစားထားသော ပြစ်မှုဆိုင်ရာ ဥပဒေများ၏ အထောက်အပံ့ ရှိမှသာ ၎င်းပြစ်မှုအား ပို၍

[7] https://privacyinternational.org/advocacy-briefing/660/privacy-internationals-response-european-commissions-public-consultation

တိတိကျကျ သတ်မှတ်ပေးခြင်း၊ ပိုမိုကျယ်ပြန့်သော အခြေအနေတွင် စဉ်းစားနိုင်ခြင်း စသည်တို့ကို ဆောင်ရွက်နိုင်မည် ဖြစ်ပြီး ပြစ်မှုအား စုံစမ်းစစ်ဆေးရန်နှင့် အရေးယူနိုင်မည့် သင့်တော်သော လုပ်ငန်းစဉ်များကို အသေးစိတ်ဖော်ပြနိုင်မည် ဖြစ်ပါသည်။

ကောင်းမွန်သော ဆိုက်ဘာမှုခင်းဥပဒေများ ပေါ်ထွန်းလာရန် ရှောင်ရမည့် အဆင့် (၃) ဆင့်

၁။ <u>အပြည်ပြည်ဆိုင်ရာ လူ့အခွင့်အရေး ဥပဒေအရ ပြစ်မှုမမြောက်သင့်သော အပြုအမူများကို ပြစ်မှုမြောက်စေရန် ချဲ့ထွင် လုပ်ဆောင်ခြင်း မပြုလုပ်ရပါ။</u>

ဥပမာအားဖြင့် ဆိုရှယ်မီဒီယာ၌ အစိုးရအား ဝေဖန်ခြင်းနှင့် မိမိတို့၏ ကိုယ်ရေးကိုယ်တာ သတင်းအချက်အလက်များကို ခိုးယူခြင်းမှ ကာကွယ်နိုင်သည့် မက်ဆေ့ပေးပို့ဝန်ဆောင်မှုများအား သုံးစွဲခြင်းတို့ ပါဝင်သည်။

၂။ <u>စောင့်ကြပ်ကြည့်ရှုခြင်း နှင့် ဆိုက်ဘာပြစ်မှုဥပဒေကို မရောယှက်ရပါ။</u>

စောင့်ကြပ်ကြည့်ရှုခြင်းသည် ရာဇဝတ်မှုများအား တားဆီးရာတွင် လိုအပ်သည် မှန်သော်လည်း ၎င်းသည် ကျူးကျော်သောလုပ်ရပ်သာ ဖြစ်ပြီး လူ့အခွင့်အရေး ချိုးဖောက်မှုများလည်း ဖြစ်ပေါ်စေနိုင်သည်။ လူ့အခွင့်အရေး ဥပဒေအရ စောင့်ကြပ်ကြည့်ရှုခြင်းသည် အချိုးအစားညီမျှပြီး လိုအပ်မှသာ အသုံးပြု၍ ဥပဒေနှင့်အညီ ဖြစ်ရန် အရေးကြီးသည်။ ဆိုက်ဘာပြစ်မှုဥပဒေတွင် စောင့်ကြပ်ကြည့်ရှုသည့်အဖွဲ့များအား တရားဝင်လုပ်ကိုင်ခွင့် ပေးလိုက်ခြင်းကြောင့် စောင့်ကြပ်ကြည့်ရှုခြင်းအား တရားဝင်ခွင့်ပြုထားသည့် ပြစ်မှုအမျိုးအစားများ အလွန်အမင်းများပြားလာနိုင်သည်။ အထူးသဖြင့် ဆိုက်ဘာနည်းလမ်းများကို အသုံးပြု၍ ကျူးလွန်သော မှုခင်းများ (Cyber enabled crimes)ကို စောင့်ကြပ်ကြည့်ရှုခွင့် တရားဝင်ပေးလိုက်လျှင် ထိုသို့ ဖြစ်လာနိုင်သည်။ နောက်ဆုံးတွင် လူများစွာ၏ ပုဂ္ဂလိကလွတ်လပ်ခွင့်ကို ကြီးမားစွာ အန္တရာယ်အယုက် ဖြစ်စေနိုင်ပြီး အထူးသဖြင့် ဥပဒေတွင် လုပ်ထုံးလုပ်နည်းဆိုင်ရာ အကာအကွယ်ပေးမှုများနှင့် အခြား လူ့အခွင့်အရေးအကာအကွယ်ပေးမှုများ မပါဝင်ပါက ဤသို့ ပိုမို ဖြစ်ပေါ်စေနိုင်သည်။ လက်ရှိကာလတွင် မြန်မာနိုင်ငံ၌ တရားဝင်သော စောင့်ကြပ်ကြည့်ရှုခြင်းနှင့် ကြားဖြတ်နားထောင်ခြင်းဆိုင်ရာ ဥပဒေတစ်ရပ် မရှိသေးပေ။ ထို့အပြင် လူ့အခွင့်အရေးကို လေးစားလိုက်နာသည့် တရားဝင် စောင့်ကြပ်ကြည့်ရှုခြင်းဆိုင်ရာ စနစ်ကို[8]

[8] လူ့အခွင့်အရေးကို လေးစားသော တရားဝင်ကြားဖြတ်အစိုးရစနစ်အတွက် မြန်မာ့စီးပွားရေးကဏ္ဍတာဝန်ယူမှုရှိရေး အထောက်အကူပြုဌာန၏မြန်မာအစိုးရသို့ အကြံပြုချက်များကိုကြည့်ပါ။ တရားဝင်ကြားဖြတ်ခြင်းနှင့် အစိုးရအနေနှင့် အသုံးပြုသူများ၏အချက်အလက်များကို ရယူခြင်း၊ "The Characteristics of a Rights-Respecting Model" နှင့် အင်္ဂလိပ်လိုအားဖြင့် Sector Wide Impact Assessment of Myanmar's ICT Sector," (2015), Recommendations – Annex, p. 35. နှင့် မြန်မာလိုအားဖြင့် Burmese တွင်ကြည့်ပါ။

ထိန်းကျောင်းပေးနိုင်မည့် လိုအပ်ချက်များလည်း မရှိသေးပေ။ ထိုစနစ်တွင် အစိုးရအဖွဲ့အစည်းများနှင့် ပုဂ္ဂလိကအဖွဲ့အစည်းများအတွက် အကျုံးဝင်သော အချက်အလက်ကာကွယ်ရေးဥပဒေတစ်ရပ် ပါဝင်သည်။[9]

၃။ <u>ထပ်ဆောင်း လူ့အခွင့်အရေးကာကွယ်ရေးဆိုင်ရာ အချက်များ မပါဝင်ပဲ ဘူတာပက်(စ်) သဘော တူညီမှုစာချုပ် (the Budapest Convention) အား ပြည်တွင်းဆိုက်ဘာပြစ်မှုဥပဒေတွင် ကူးယူ ဖော်ပြခြင်း မပြုလုပ်ရပါ။</u>

ဘူတာပက်(စ်) သဘောတူညီမှုစာချုပ် (the Budapest Convention)ရှိ ပြဋ္ဌာန်းချက်များအား လူ့အခွင့်အရေးကာကွယ်ပေးမှုများဖြင့် ထောက်ပံ့ဖြည့်ဆည်းပေးရမည်။

ဘူတာပက်(စ်) သဘောတူညီမှုစာချုပ် (the Budapest Convention)- အီးယူကောင်စီ၏ ၂၀၀၁ ခုနှစ် ဆိုက်ဘာမှုခင်း သဘောတူညီမှုစာချုပ်

အီးယူကောင်စီ၏ ၂၀၀၁ ခုနှစ် ဆိုက်ဘာမှုခင်း သဘောတူညီမှုစာချုပ် (ဘူတာပက်(စ်) သဘောတူညီမှုစာချုပ်)သည် ဆိုက်ဘာမှုခင်းဆိုင်ရာ အပြည်ပြည်ဆိုင်ရာ ပူးပေါင်းပါဝင်မှုအတွက် မူဘောင်တစ်ရပ် ဖြစ်သည်။[10] ထိုစာချုပ်သည် ဆိုက်ဘာမှုခင်းအား အရေးယူနိုင်မည့် ပြည်တွင်းဥပဒေကို ပြဋ္ဌာန်းနေသည့် နိုင်ငံတိုင်းအတွက် လမ်းညွှန်ချက်အနေဖြင့် ဖြည့်ဆည်းပေးရန် ဖြစ်သော်လည်း ၎င်းအချက်များကို လွန်ခဲ့သော နှစ်ပေါင်း (၂၀) ခန့်က ရေးသားထားခြင်းဖြစ်သည်ကို တွေ့ရသည်။ နိုင်ငံများအနေနှင့် ဆိုက်ဘာမှုခင်းဥပဒေများ ရေးဆွဲရာတွင် ဤသဘောတူညီမှုစာချုပ်ကို အခြေခံအဖြစ် မှီငြမ်းကြောင်း တွေ့ရှိရသည်။

ဤသဘောတူညီမှုစာချုပ်၏ အရေးပါသော အချက် (၃) ချက်မှာ -

(၁) ပါဝင်ဆောင်ရွက်နေသော နိုင်ငံအသီးသီးမှ ပြဋ္ဌာန်းထားသင့်သည့် ပြစ်မှုများ၏ စာရင်းအား ပြုစုခြင်း
(၂)ဆိုက်ဘာမှုခင်းများအား စုံစမ်းစစ်ဆေးရန်အတွက် အခွင့်အာဏာရှိ အဖွဲ့အစည်း၊ ပုဂ္ဂိုလ် အသစ်များ လိုအပ်နေခြင်း
(၃)ဆိုက်ဘာမှုခင်းနှင့်ပတ်သက်သည့် နယ်စပ်ဖြတ်ကျော် အထောက်အပံ့များ ကူညီဆောင်ရွက်ပေးခြင်း တို့ဖြစ်သည်။

[9] မြန်မာ့စီးပွားရေးကဏ္ဍတာဝန်ယူမှုရှိရေး အထောက်အကူပြုဥပဒေ၏ လုံခြုံရေးနှင့်အချက်အလက် ကာကွယ်ရေးနှင့်ပတ်သတ်သော တွဲဖက်မူဝါဒရေးရာအကျဉ်းချုပ်

[10] Council of Europe, The Convention on Cyber Crime of the Council of Europe, (CETS No. 185), known as The Budapest Convention.

ဤစာချုပ်သည် အီးယူ လူ့အခွင့်အရေးဆိုင်ရာ သဘောတူညီမှုစာချုပ်နှင့် အီးယူအချက်အလက် ကာကွယ်ရေး ဥပဒေ (General Data Protection Regulation)တို့ကို လိုက်နာကျင့်သုံးရမည်ဖြစ်သော EU နိုင်ငံများတွင် အကောင်အထည်ဖော်ရန် ချုပ်ဆိုထားသော စာချုပ်ဖြစ်သည်။ ထို့ကြောင့် ဤသဘောတူညီမှု စာချုပ်အား ပိုမိုကျယ်ပြန့်သည့် ဥပဒေဆိုင်ရာ စနစ်ပါ လူ့အခွင့်အရေး အကာအကွယ်များဖြင့် ဖြည့်ဆည်းထောက်ပံ့ပေးမည်ဟု ယူဆရသည်။ ထို့အပြင် စာချုပ်ပါ အပိုဒ် ၁၅ အရ ဥရောပ လူ့အခွင့်အရေးဆိုင်ရာ သဘောတူညီမှုစာချုပ်၊ နိုင်ငံတကာ ပြည်သူနှင့် နိုင်ငံရေး အခွင့်အရေးများဆိုင်ရာ ပဋိညာဉ်စာချုပ်၊ အခြား သက်ဆိုင်သော နိုင်ငံတကာ လူ့အခွင့်အရေးဆိုင်ရာ ပြဋ္ဌာန်းချက်များနှင့် အချိုးညီမျှမှု၏ နိယာမ (the principal of proportionality) စသည်တို့နှင့် အလားတူညီမျှသော လူ့အခွင့်အရေးဆိုင်ရာ အကာအကွယ်ပေးခြင်းများဖြင့်လည်း ထောက်ပံ့ဖြည့်ဆည်းပေးရမည်ဟု ရှင်းရှင်းလင်းလင်း ဖော်ပြထားသည်။[11] သို့သော်လည်း လောလောဆယ်၌ မြန်မာနိုင်ငံ၏ ကျယ်ပြန့်သော ဥပဒေစနစ်တွင် ထိုအကာအကွယ်ပေးမှုများ မရှိသေးပေ။ သို့ဖြစ်ရာ ဆိုက်ဘာလုံခြုံရေးနှင့် ဆိုက်ဘာမှုခင်းဆိုင်ရာ မြန်မာ့ဥပဒေသစ်များကို ရေးဆွဲရာတွင် ဘူတာပက်(စ်) သဘောတူညီမှုစာချုပ်ရှိ အဓိကအချက်များကို ဖြေရှင်းခြင်းအပြင် အထက်ပါ အကာအကွယ်ပေးမှုများကို ထည့်သွင်းပေါင်းစပ်ခြင်း ပြုလုပ်သင့်ပါသည်။

[11] Council of Europe, Practical Guide on the use of personal data in the police sector: how to protect personal data while combatting crime, 15 February 2018.