ပြည်သူ့လွှတ်တော်ရုံး
သူတေသနဌာန

ရက်စွဲ ။ ၂၀၁၈ ခုနှစ် ၊ ဇွန်လ ၁၈ ရက်

ဆိုက်ဘာလုံခြုံရေးမှ သတိပြုဖွယ်ရာ ကောက်နှုတ်ချက်များ

အကျဉ်းချုပ်

ဆိုက်ဘာလုံခြုံရေးကို အင်တာနက်အပါအဝင် ကွန်ပျူတာကွန်ရက်များ၏ လုံခြုံရေးဟု လွယ်ကူစွာနားလည်နိုင်ပါသည်။ နိုင်ငံတစ်နိုင်ငံက အခြားသောနိုင်ငံ၏ ကွန်ပျူတာကွန်ရက်များကိုဖျက်ဆီးရန် သို့မဟုတ် နှောင့်ယှက်ရန်အတွက် ဝင်ရောက်တိုက်ခိုက်ဖျက်ဆီးမှုသည် ဆိုက်ဘာတိုက်ခိုက်မှု ဖြစ်သကဲ့သို့ နိုင်ငံမဟုတ်သည့် အကြမ်းဖက်အုပ်စုများ၊ နိုင်ငံရေးအစွန်းရောက်အဖွဲ့အစည်းများနှင့် နိုင်ငံတကာပြစ်မှုဆိုင်ရာ အဖွဲ့အစည်းများသည် မကောင်းသတင်းများဖြန့်ဝေခြင်း၊ ဝါဒဖြန့်ဝေခြင်းများသည်လည်း ဆိုက်ဘာတိုက်ခိုက်မှုပင်ဖြစ်ပါသည်။ ယခင်စစ်အေးခေတ်ကာလတွင် ထိပ်တန်းလက်နက်မှာ နျူကလီးယား ပဲ့ထိန်းဒုံးကျည်များဖြစ်ပါသည်။ ယနေ့ခေတ်တွင် ဆော့ဖ်ဝဲလ်၊ ကွန်ပျူတာစနစ်များကို တိုက်ခိုက်ရာတွင်လည်းကောင်း၊ မျက်မြင်ရှိနေသည့် ကမ္ဘာကြီးအတွင်းမှပစ်မှတ်များကို တိုက်ခိုက်ရာတွင်လည်းကောင်း ဆော့ဖ်ဝဲလ်များကို အသုံးပြုကြသည်။ ကုမ္ပဏီများ၊ လျှပ်စစ်ဓာတ်အားပေးစက်ရုံများ၊ ဘဏ်များ၊ ဆေးရုံများနှင့် သယ်ယူပို့ဆောင်ရေးစနစ်များကို ဆိုက်ဘာတိုက်ခိုက်မှုများ လုပ်ဆောင်နေကြသည်။ အမေရိကန်ပြည်ထောင်စုရွေးကောက်ပွဲကိုပင် တိုက်ခိုက်ခဲ့ကြသည်။ သို့ဖြစ်၍ ဆိုက်ဘာလုံခြုံရေးသည် သာမန်ကဏ္ဍတစ်ခုသာမက နိုင်ငံတော်နှင့်နိုင်ငံသားများ၏အကျိုးစီးပွားနှင့် တိုက်ရိုက်ဆက်စပ်နေသည့် အမျိုးသားလုံခြုံရေးကဏ္ဍတစ်ရပ် ဖြစ်လာပါသည်။

သုတေသနစာတမ်းတို အမှတ်စဉ် (၈၄)

မာတိကာ

နိဒါန်း

၁။ နည်းပညာဖွံ့ဖြိုးမှုနှင့်အတူ နိုင်ငံများ၏အမျိုးသားအကျိုးစီးပွားသည် ပြင်ပကမ္ဘာထက် Virtual World ဖြစ်သော ဆိုက်ဘာကမ္ဘာပေါ်သို့ ဦးတည်နေပြီဖြစ်သောကြောင့် ပြိုင်ဘက်နိုင်ငံများ၊ အဖွဲ့အစည်းများ၏တိုက်ခိုက်လာမည့်အန္တရာယ်မှ ကောင်းစွာကာကွယ်နိုင်ရန် ပြင်ဆင်ဖို့လိုအပ်လာပါသည်။အနာဂတ်တွင် နိုင်ငံများအကြား စစ်ဆင်မှုများသည် သမားရိုးကျစစ်ဆင်မှုများနှင့်အတူ ဆိုက်ဘာစစ်ဆင်မှုများလည်း ပေါင်းစပ်ကျင့်သုံး၍ တိုက်ခိုက်နိုင်ဖွယ်ရှိကြောင်း ပညာရှင်များက သုံးသပ်ထားကြသည်။ သို့ဖြစ်၍ အချို့သောနိုင်ငံများရှိ တပ်မတော်၏ဖွဲ့စည်းပုံတွင် ဆိုက်ဘာတပ်ဖွဲ့များကိုဖွဲ့စည်းကာ ခုခံကာကွယ်နိုင်ရေးအတွက် ပြင်ဆင်ဆောင်ရွက်လျက် ရှိနေကြသည်ကို တွေ့ရှိရပါသည်။

ဆိုက်ဘာလုံခြုံရေးအဓိပ္ပါယ်

၂။ ဆိုက်ဘာလုံခြုံရေးဆိုသည်မှာ အဖွဲ့အစည်းများနှင့် အသုံးပြုသူများ၏ပိုင်ဆိုင်မှုများကို ကာကွယ်ရန်အတွက် ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ ကိရိယာများ၊ ချမှတ်ရန်လိုအပ်သော ဆိုက်ဘာလုံခြုံရေးနည်းလမ်းများ၊ ညွှန်ကြားချက်များ၊ လုပ်ထုံးလုပ်နည်းများ၊ နည်းပညာများနှင့်လက်တွေ့ကျင့်သုံးရန် နည်းလမ်းကောင်းများ အသုံးပြုခြင်းကို ဆိုလိုပါသည်။ အဖွဲ့အစည်းများနှင့် အသုံးပြုသူများ၏ပိုင်ဆိုင်မှုများဟုဆိုရာတွင် အသုံးပြုရန်ချိတ်ဆက်ထားသောကိရိယာများ၊ ဝန်ဆောင်မှုများ၊ ကွန်ယက်စနစ်များ၊ ဆက်သွယ်ရေးဆိုင်ရာမီဒီယာများ၊ ဆိုက်ဘာအဖွဲ့အစည်းတွင် သိမ်းဆည်းမည့် သတင်းအချက်အလက်များနှင့် ပို့လွှတ်မည့်သတင်း အချက်အလက်များ ပါဝင်ပါသည်။

ဆိုက်ဘာလုံခြုံရေး လုပ်ဆောင်ရခြင်း၏ ရည်ရွယ်ချက်

၃။ ဆိုက်ဘာလုံခြုံရေးလုပ်ဆောင်ရခြင်း၏ ရည်ရွယ်ချက်များမှာ ဆိုက်ဘာအဖွဲ့အစည်းများအတွင်း အသုံးပြုသူများ၏ လျှို့ဝှက်သောသတင်းအချက်အလက်များနှင့် ပိုင်ဆိုင်မှုများကို လုံခြုံစိတ်ချစွာထိန်းသိမ်းနိုင်ရေး၊ အသုံးပြုနိုင်ရေး၊ ညီညွတ်မှန်ကန်စွာအသုံးပြုနိုင်ရေး၊ အပြန်အလှန်ယုံကြည်စွာဖလှယ်နိုင်ရေး၊ ဖြန့်ဝေနိုင်ရေးနှင့် ကွန်ယက်လုံခြုံရေးတို့ ပါဝင်ပါသည်။

ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ စံသတ်မှတ်ချက်များ

၄။ ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ တိုက်ခိုက်မှုများကို လျော့ချနိုင်ရန်အတွက် ကမ္ဘာနှင့်အဝှမ်း လက်တွေ့အသုံးပြုနေသော နည်းလမ်းများနှင့် စံသတ်မှတ်ချက်များကို ဆိုလိုပါသည်။ ထိုစံသတ်မှတ်ချက်များတွင် ယေဘုယျစံသတ်မှတ်ချက်များနှင့် ဆိုက်ဘာလုံခြုံရေး အကောင်အထည်ဖော်နိုင်ရန် အသေးစိတ်အချက်အလက်များ၊ အသုံးပြုမည့် နည်းဗျူဟာများနှင့် ၎င်းတို့ကို အကောင်အထည်ဖော်ရာတွင် အသုံးပြုရမည့်နည်းပညာများ ပါဝင်ပါသည်။ စံသတ်မှတ်နိုင်ရန် အခွင့်အာဏာရှိသော စံသတ်မှတ်ရေးအဖွဲ့အစည်းများ၏ ထောက်ခံချက် ရရှိပြီးမှသာလျှင် ဆိုက်ဘာလုံခြုံရေးစံအဖြစ် သတ်မှတ်နိုင်ပါသည်။ စံသတ်မှတ်ချက်အနေဖြင့်-

(က) စီးပွားရေးဆိုင်ရာ သတင်းအချက်အလက် ဆက်သွယ်ဆောင်ရွက်ချက်များအတွက် နိုင်ငံတကာစံသတ်မှတ်ချက်မှာ ISO 27031 (FCI)၊

(ခ) ဆိုက်ဘာလုံခြုံရေး စီမံကိန်းများအတွက် နိုင်ငံတကာစံသတ်မှတ်ချက်မှာ ISO 27031 (CD)၊

(ဂ) ကွန်ယက်ဆိုင်ရာ လုံခြုံရေး စီမံကိန်းများအတွက် ISO 27031 (FDIS)၊

(ဃ) အသုံးချရမည့် လုပ်ငန်းဆိုင်ရာ လုံခြုံရေးများအတွက် ISO 27031 (CD)၊

(င) သတင်းအချက်အလက် လုံခြုံရေးဆိုင်ရာ ဖြစ်ပွားမှုများကို စီမံခန့်ခွဲပေးခြင်းများအတွက် ISO 27031 (FCD)၊

(စ) သတင်းအချက်အလက် လုံခြုံမှုစီမံခန့်ခွဲရေးအတွက် လမ်းညွှန်မှု စံသတ်မှတ်ချက် ISO IEC TR 13335 (GMITS) တို့ဖြစ်ပါသည်။

ဆိုက်ဘာလုံခြုံရေး တိုက်ခိုက်မှု အမျိုးအစားများ

၅။ ဆိုက်ဘာလုံခြုံရေး တိုက်ခိုက်မှုအမျိုးအစားများကို ဖော်ပြပါအတိုင်း သတ်မှတ်နိုင်ပါသည်-

(က) Hacking (သက်ဆိုင်သူ တစ်ဦးတစ်ယောက်၏ ခွင့်ပြုချက်မရှိဘဲ မသမာသော လုပ်ဆောင်ချက်များပြုလုပ်ခြင်း၊ ဥပမာ- သတင်းအချက်အလက်များခိုးယူခြင်း)

(ခ) Denial of Service Attack(အသုံးပြုရမည့်သူများ အသုံးမပြုနိုင်ရန် လုပ်ဆောင်ခြင်း)

(ဂ) Virus Dissemination (ကွန်ပျူတာ virus များ ပြန့်ပွားစေခြင်း)

(ဃ) Software Privacy (ခွင့်ပြုချက်လိုင်စင်မရှိဘဲ အသုံးပြုခြင်း)

(င) IRC Crime (Internet Chat Room များမှ မသမာမှုများ ပြုလုပ်ခြင်း)

(စ) Credit Card Fraud (Credit Card Number များကို ပိုင်ရှင်မသိဘဲ ခိုးယူခြင်း)

(ဆ) Net Extortion (Internet ကို အသုံးပြု၍ ခြိမ်းခြောက်၍ ငွေညစ်ခြင်း)

(ဇ) Phishing (အရေးကြီးစီးပွားရေးဆိုင်ရာ အချက်အလက်များကို ခိုးယူခြင်း)

(ဈ) Spoofing (အပြောင်အပျက်သဘောဖြင့် လှည့်ဖြားခြင်း - အခြားသူများ၏ IP Address များကို ခိုးယူသုံးစွဲခြင်း)

(ည) Cyber Stalking (Internet Email အစရှိသည့် မီဒီယာများကို အသုံးပြု၍ နောက်ယောင်ခံလိုက်ခြင်း)

(ဋ) Cyber Defamation (အသရေဖျက်ခြင်း-Internet Email အစရှိသည့် မီဒီယာများကို အသုံးပြု၍ မကောင်းသတင်းလွှင့် တိုက်ခိုက်ခြင်း)

(ဌ) Threatening (Internet Email အစရှိသည့် မီဒီယာများကို အသုံးပြု၍ ခြိမ်းခြောက်ခြင်း)

(ဍ) Salami Attack (Bank Server တွင် သုံးစွဲသူများ၏ ငွေ Account များမှ မသိမသာထုတ်ယူနိုင်သော software များထည့်သွင်းထားခြင်း) တို့ပါဝင်ပါသည်။

ဆိုက်ဘာသုံးစွဲသူများ သတိပြုလိုက်နာရမည့်အချက်များ

၆။ ဆိုက်ဘာသုံးစွဲသူများ သတိပြုလိုက်နာရမည့် အချက်များမှာ-

(က) မိမိတို့သုံးစွဲသောကွန်ပျူတာကို နောက်ဆုံးပေါ် Virus ကာကွယ်ပေးသော Software များကို သုံးစွဲသင့်ပါသည်။ ၎င်း Software များကိုလည်း အမြဲ Update လုပ်ပေးရပါမည်။

(ခ) မိမိတို့၏သတင်းအချက်အလက်များ လုံခြုံစေရန်အတွက် သူတစ်ပါးအလွယ်တကူ မခန့်မှန်းနိုင်သော မိမိ၏စနစ်တွင်းသို့ဝင်မည့် Password များကို အသေအချာ ပေးသင့်ပါသည်။

(ဂ) အနည်းဆုံးရက် ၉၀ လျှင်တစ်ကြိမ် အသစ်ပြန်လည်ပြောင်းသင့်ပါသည်။ Password များပေးလျှင်လည်း မိမိတို့ကိုယ်ရေးကိုယ်တာများနှင့် သက်ဆိုင်သောအမည်များ၊ တယ်လီဖုန်းနံပါတ်များ၊ မွေးနေ့ ရက်စွဲများ၊ Credit Card နံပါတ်များ ၊ လိပ်စာများ စသည်ဖြင့် မပေးသင့်ပါ။

(ဃ) သကေ်တများ၊ ဂဏာန်းများ၊ အက္ခရာအကြီးအသေးများ ပေါင်းစပ်၍ မိမိတို့၏ Password များကို ပေးသင့်ပါသည်။

(င) မိမိကွန်ပျူတာတွင် အခြား Device များကိုမသုံးစွဲမီ ထိုပစ္စည်းများ ဗိုင်းရက်စ် ကင်းစင်စေရန်လည်း ပြုလုပ်ရပါမည်။

(စ) အကယ်၍ ဗိုင်းရပ်စ်တွေ့ရှိခဲ့လျှင်လည်း စနစ်ထိန်းချုပ် ကွပ်ကဲသူသို့ ချက်ချင်း အကြောင်းကြားသင့်ပါသည်။

(ဆ) ဆိုက်ဘာလုံခြုံရေးထိခိုက်နိုင်သည့် ဖြစ်စဉ်များ ဖြစ်ပွားပါက သက်ဆိုင်ရာ ဆိုက်ဘာ လုံခြုံရေးအဖွဲ့ကို ချက်ချင်း အကြောင်းကြားသင့်ပါသည်။

(ဇ) မိမိကွန်ပျူတာမှ အဝေးသို့ မထွက်ခွာမီ မိမိအကောင့်မှ ထွက်ခဲ့ရန်နှင့် အပြင်သို့ မထွက်ခွာမီ မိမိကွန်ပျူတာကို ပိတ်ထားခဲ့ရမည်။[1]

ဆိုက်ဘာလုံခြုံရေးအဆင့် တိုင်းတာသည့် မဏ္ဍိုင် (၅) ရပ်

၇။ အာဆီယံနိုင်ငံများ၏ဆိုက်ဘာလုံခြုံရေးအဆင့်နှင့် နှိုင်းယှဉ်လေ့လာကြည့်ပါက မြန်မာနိုင်ငံသည် များစွာနောက်ကျနေပြီး ဖွံ့ဖြိုးတိုးတက်ရန်အတွက် အားသွန်ဆောင်ရွက်ရန်လိုအပ်နေပါသည်။ ကုလသမဂ္ဂအောက်ရှိ အဖွဲ့အစည်းတစ်ခုဖြစ်သော နိုင်ငံတကာသတင်းနှင့် ဆက်သွယ်ရေးသမဂ္ဂ (International Telecommunication Union- ITU) က အဖွဲ့ဝင်နိုင်ငံပေါင်း ၁၉၅ နိုင်ငံ၏ ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ ပြင်ဆင်ဆောင်ရွက်ထားရှိမှုအား အကဲဖြတ်အမှတ်ပေးကာ “၂၀၁၇ ခုနှစ် ဆိုက်ဘာလုံခြုံရေးအညွှန်းကိန်း”ကို ထုတ်ပြန်ခဲ့ပါသည်။ နိုင်ငံများ၏ ဆိုက်ဘာလုံခြုံရေး အညွှန်းကိန်းကို တိုင်းတာရာတွင် မဏ္ဍိုင်ကြီး (၅)ရပ်အပေါ် အခြေခံတိုင်းတာပြီး အဆိုပါ မဏ္ဍိုင်ကြီး (၅) ရပ်မှာ ဖော်ပြပါအတိုင်းဖြစ်ပါသည်-

[1] Available from: https://www.mmcert.org.mm/node/163 [accessed 25 April 2018]

(က) ဥပဒေဆိုင်ရာ (Legal)

(ခ) နည်းပညာဆိုင်ရာ (Technical)

(ဂ) အဖွဲ့အစည်းဆိုင်ရာ (Organizational)

(ဃ) လူသားစွမ်းရည်မြှင့်တင်မှုဆိုင်ရာ (Capacity Building)

(င) ပူးပေါင်းဆောင်ရွက်မှုဆိုင်ရာ (Cooperation) တို့ဖြစ်ပါသည်။

၈။ ဥပဒေဆိုင်ရာတိုင်းတာမှုတွင် ဆိုက်ဘာရာဇဝတ်မှုဆိုင်ရာဥပဒေများ၊ ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ စည်းမျဉ်းစည်းကမ်းများနှင့် ဆိုက်ဘာလုံခြုံရေးလေ့ကျင့်သင်ကြားမှုများနှင့် သက်ဆိုင်သည့် ဥပဒေများရေးဆွဲထားခြင်း ရှိ၊မရှိ၊ ခိုင်မာအားကောင်းမှု ရှိ၊မရှိ စသည်တို့ကို အကဲဖြတ်ခြင်းဖြစ်ပါသည်။ နည်းပညာပိုင်းဆိုင်ရာ အကဲဖြတ်ရာတွင် ကွန်ပျူတာဖြစ်စဉ်များကို တုန့်ပြန်မှုအဖွဲ့များ CIRT (Computer Incidents Response Team) အဖွဲ့များနှင့် မြန်မာနိုင်ငံကွန်ပျူတာအရေးပေါ် တုန့်ပြန်မှုအဖွဲ့ mmCERT (Myanmar Computer Emergency Response Team) များကို နိုင်ငံတော်အဆင့်၊ ဒေသန္တရအဆင့်၊ ဌာနအဖွဲ့အစည်းအဆင့်စသည်ဖြင့် ဖွဲ့စည်းဆောင်ရွက်နေမှုအခြေအနေများ၊ ဆိုက်ဘာအဖွဲ့အစည်းများဖွဲ့စည်းရန် စံသတ်မှတ်ချက်များ၊ ဆိုက်ဘာကျွမ်းကျင်ပညာရှင်ဆိုင်ရာ စံနှုန်းသတ်မှတ်ချက်များ၊ ကလေးသူငယ်များကို ဆိုက်ဘာလုံခြုံမှုရှိရန် ကာကွယ်ဆောင်ရွက်ထားမှုများ စသည်တို့ကိုတိုင်းတာအကဲဖြတ်ပါသည်။ အဖွဲ့အစည်းဆိုင်ရာ တိုင်းတာရာတွင် ဖွဲ့စည်းထားရှိသည့်အဖွဲ့များ၏ မဟာဗျူဟာချမှတ်ဆောင်ရွက်နေမှု၊ ဆိုက်ဘာလုပ်ငန်းအတွက် တာဝန်ရှိသည့်အဖွဲ့အစည်းများ ဖွဲ့စည်းထားရှိမှုနှင့် ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ ရှုထောင့်များဖြင့် တိုင်းတာအမှတ်ပေးပါသည်။

၉။ လူသားစွမ်းရည်မြှင့်တင်မှုဆိုင်ရာ ကဏ္ဍတွင် စံသတ်မှတ်ရေးအဖွဲ့များ ဖွဲ့စည်းထားရှိမှု၊ ကောင်းမွန်သည့် အလေ့အထများကျင့်သုံးမှု၊ သုတေသနဆောင်ရွက်နေမှုအခြေအနေများ၊ အများပြည်သူသို့ ပညာပေးဆောင်ရွက်မှု၊ ဆိုက်ဘာကျွမ်းကျင်ပညာရှင်များ လေ့ကျင့်ပို့ချထောင်နေမှု၊ အမျိုးသားပညာရေးတွင် ထည့်သွင်းပါဝင်မှုနှင့် ကျောင်းသင်ရိုးညွှန်းတမ်းများတွင် ထည့်သွင်းသင်ကြားပေးမှုအခြေအနေများ၊ မက်လုံးပေး၊ အားပေးဆောင်ရွက်နေမှုအခြေအနေများနှင့် အခြားနိုင်ငံများမှ ကူးယူခြင်းမပြုဘဲ မိမိနိုင်ငံတွင် တီထွင်ဖော်ထုတ်နိုင်မှုအခြေအနေများ စသည်တို့အပေါ်

မူတည်ကာ တိုင်းတာအမှတ်ပေးပါသည်။ ပူးပေါင်းဆောင်ရွက်မှုဆိုင်ရာကဏ္ဍတွင် နိုင်ငံများအကြား သဘောတူစာချုပ်များ ချုပ်ဆိုဆောင်ရွက်နေမှုအခြေအနေများ၊ နိုင်ငံတကာတွင်ပူးပေါင်းဆောင်ရွက်နေသည့်အခြေအနေများ၊ အစိုးရအနေဖြင့် ဆိုက်ဘာလုပ်ငန်းများတွင် ပုဂ္ဂလိကကဏ္ဍနှင့်ပူးပေါင်းဆောင်ရွက်နေသည့်အခြေအနေများ၊ နိုင်ငံရှိဆိုက်ဘာအဖွဲ့အစည်းများအကြား ပူးပေါင်းဆောင်ရွက်မှုအခြေအနေများစသည်တို့ကို အကဲဖြတ်တိုင်းတာခြင်းဖြစ်ပါသည်။

နိုင်ငံအလိုက် ဆိုက်ဘာလုံခြုံမှုအဆင့်များ

၁၀။ အထက်ပါတိုင်းတာချက်များအရ စင်ကာပူနိုင်ငံသည် ကမ္ဘာ့အဆင့်နံပါတ် ၁ တွင် ရှိနေပါသည်။ အမေရိကန်နိုင်ငံသည် ဒုတိယအဆင့်တွင်ရှိပြီး နောက်တွင် အာဆီယံနိုင်ငံတစ်ခုဖြစ်သည့် မလေးရှားနိုင်ငံသည် တတိယအဆင့်တွင်ရှိသည်ကို တွေ့ရှိရပါသည်။ မြန်မာနိုင်ငံ၏အိမ်နီးချင်းနှင့် ဒေသတွင်းနိုင်ငံများကို လေ့လာကြည့်ရာတွင် ထိုင်းနိုင်ငံ အဆင့် (၂၀)၊ အိန္ဒိယ အဆင့်(၂၁)၊ တရုတ် အဆင့်(၃၂)၊ ဖိလစ်ပိုင် အဆင့် (၃၇)၊ ဘရူနိုင်း အဆင့်(၅၃)၊ ဘင်္ဂလားဒေ့ရှ် အဆင့်(၅၃)၊ အင်ဒိုနီးရှား အဆင့် (၇၀)၊ သီရိလင်္ကာ အဆင့်(၇၂)၊ လာအို အဆင့်(၇၇)၊ ကမ္ဘောဒီးယား အဆင့် (၉၂)၊ ဗီယက်နမ် အဆင့် (၁၀၁)နှင့် အရှေ့တီမော အဆင့် (၁၆၂) အသီးသီးရှိကြောင်း တွေ့ရှိရပါသည်။ မြန်မာနိုင်ငံသည် အဆင့် (၁၀၀)တွင် ရှိနေရာ အာဆီယံနှင့် ဒေသတွင်းတွင် မြန်မာနိုင်ငံ၏ နောက်၌ ဗီယက်နမ်နှင့် အရှေ့တီမောတို့သာရှိကြောင်း လေ့လာတွေ့ရှိရပါသည်။ သို့သော် မကြာသေးမီလပိုင်းအတွင်းက ဗီယက်နမ်နိုင်ငံသည် ဆိုက်ဘာလုံခြုံရေးကဏ္ဍ တိုးတက်မြင့်မားရေးအတွက် ဆိုက်ဘာတပ်ဖွဲ့တစ်ခု ဖွဲ့စည်းဆောင်ရွက်ကာ တပ်ဖွဲ့ဝင် ၁၀၀၀၀ ခန့်အထိ ခန့်အပ် တာဝန်ပေးထားသည်ကို တွေ့ရှိရ၍ ဗီယက်နမ်နိုင်ငံ၏ ဆိုက်ဘာလုံခြုံရေးကြိုးပမ်းမှုများသည် လက်တွေ့တွင် မြန်မာနိုင်ငံထက် သာလွန်နိုင်ပြီဖြစ်ပါသည်။[2]

မြန်မာနိုင်ငံတွင် လက်ရှိဆောင်ရွက်ချက်များ

၁၁။ မြန်မာနိုင်ငံအနေဖြင့် ဆိုက်ဘာလုံခြုံရေးနှင့် သတင်းအချက်အလက်လုံခြုံရေးကို အထူးအလေးထား ဆောင်ရွက်နိုင်ရန်အတွက် နိုင်ငံတော်၏အတိုင်ပင်ခံပုဂ္ဂိုလ် ဒေါ်အောင်ဆန်းစုကြည်မှ

[2] e-Government နှင့် ဆိုက်ဘာလုံခြုံရေး၊ တည်ကြည်မောင်၊ ၂၀၁၈ ခုနှစ်၊ ဖေဖော်ဝါရီလ ၂၀ ရက်နေ့ထုတ် ကြေးမုံသတင်းစာ၊ စာမျက်နှာ ၆ မှ ကောက်နှုတ်ထားပါသည်။(ကြည့်ရှုသည့်ရက် ၂၀-၂-၂၀၁၈)

နာယက ၊ ဒုတိယသမ္မတဦးမြင့်ဆွေမှ ဥက္ကဋ္ဌ အဖြစ်ပါဝင်သော e-Government ဦးဆောင်ကော်မတီ အား ၂၀၁၈ ခုနှစ်၊ ဇန်နဝါရီလတွင် ဖွဲ့စည်းပြီးဖြစ်ပါသည်။[3]

၁၂။ ပို့ဆောင်ရေးနှင့် ဆက်သွယ်ရေးဝန်ကြီးဌာနအနေဖြင့် သတင်းအချက်အလက်နည်းပညာနှင့် ဆိုက်ဘာလုံခြုံရေးဦးစီးဌာနကို ၂၀၁၅ခုနှစ်၊ ဧပြီလ(၁)ရက်နေ့တွင် စတင်၍တည်ထောင်ဖွဲ့စည်းခဲ့ပါသည်။ဌင်းဦးစီးဌာနအနေဖြင့် ဌာနဆိုင်ရာအသီးသီးမှ အကောင်အထည်ဖော်ဆောင်ရွက်ထားသည့် e-Government လုပ်ငန်းစဉ်များအား အကျိုးရှိရှိပေါင်းစပ်အသုံးပြုနိုင်ရေး၊ လုပ်ငန်းစဉ်အသစ်များအားလေ့လာ၍ စီမံကိန်းအသစ်များရေးဆွဲအကောင်အထည်ဖော်ဆောင်ရေး၊ သတင်းအချက်အလက်ဆက်သွယ်ရေးနည်းပညာ(ICT)စံနှုန်းများသတ်မှတ်နိုင်ရေး၊ လိုအပ်သည့်ဥပဒေများပြဌာန်းနိုင်ရေး၊ ပြဌာန်းထားသည့်ဥပဒေနှင့်အညီ သတင်းအချက်အလက် ဆက်သွယ်ရေးနည်းပညာနှင့်ဆိုက်ဘာလုံခြုံရေးလုပ်ငန်းများ စနစ်တကျကြီးကြပ်၍ အကောင်အထည်ဖော် ဆောင်ရွက်နိုင်ရေးနှင့် အဖွဲ့အစည်း၊ ဌာနဆိုင်ရာအချင်းချင်းတို့အား ညှိနှိုင်းဆောင်ရွက်ပေးနိုင်ရေးတို့အတွက် ရည်ရွယ်၍ အောက်ဖေါ်ပြပါဌာနခွဲ(၆)ခုဖြင့် တည်ထောင် ဖွဲ့စည်းခဲ့ခြင်းဖြစ်ပါသည်-

(က) စီမံ/ဘဏ္ဍာ/ထောက်ပံ့ရေးဌာန

(ခ) e-Government ဌာန

(ဂ) ဥပဒေ/နိုင်ငံတကာ/ပြန်ကြားရေးဌာန

(ဃ) National Cyber Security Center

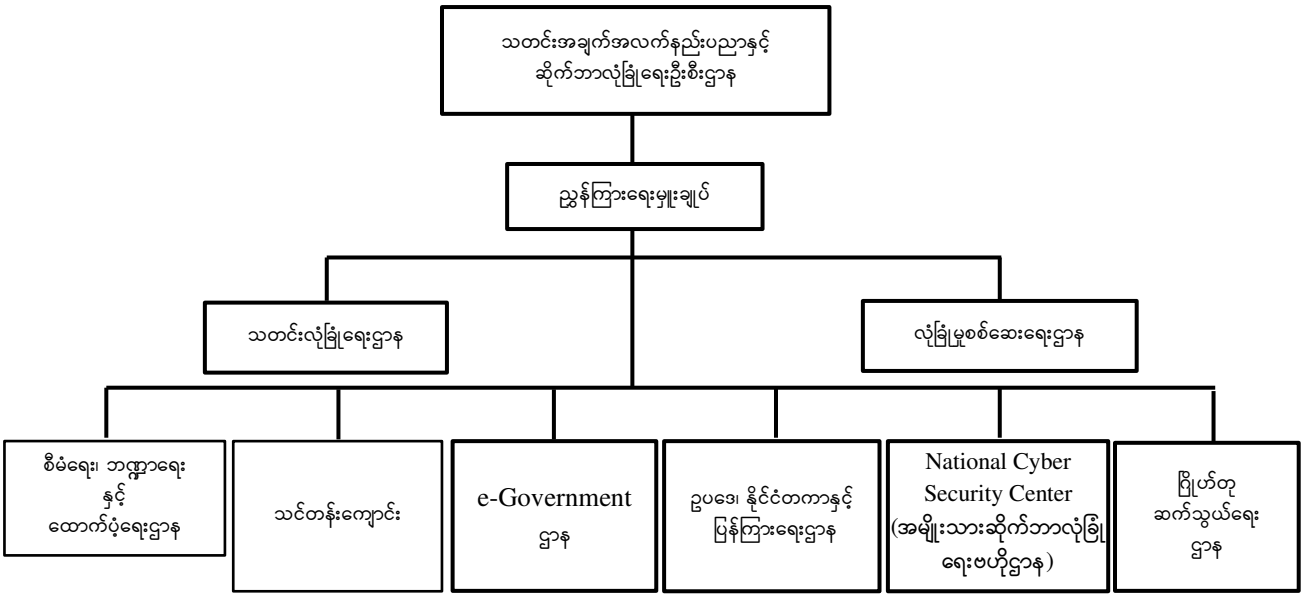
(င) ဂြိုဟ်တုဆက်သွယ်ရေးဌာန

(စ) သင်တန်းကျောင်း[4]

[3] Available from: http://thevoicemyanmar.com/tags/e-Government/posts/18269-egn [accessed 7 march 2018]

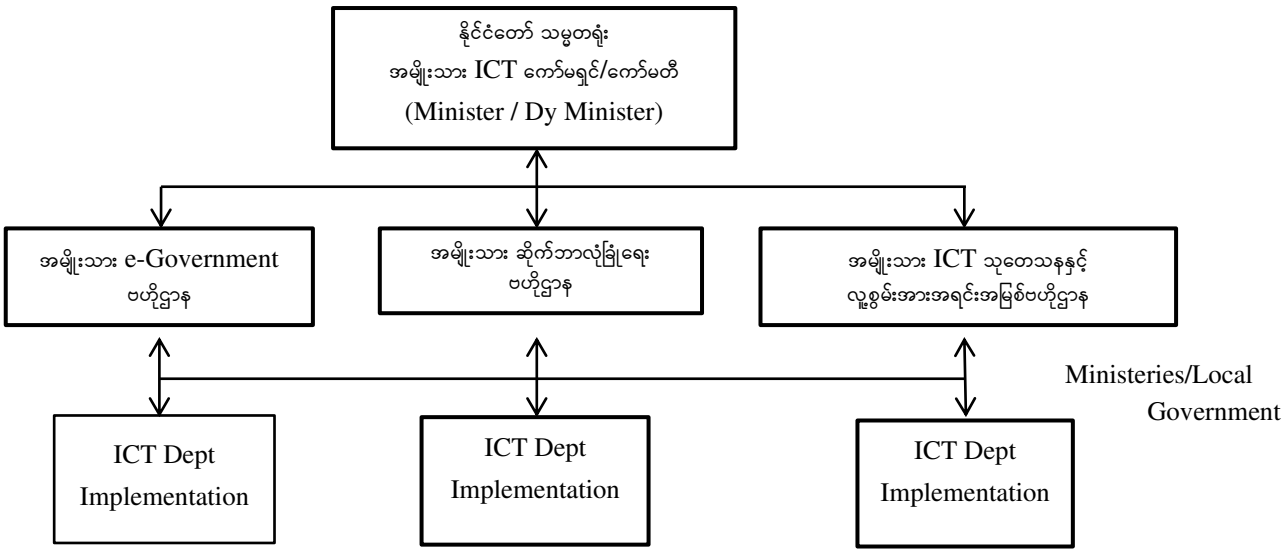
[4] Available From : https://tinyurl.com/ybpyy7sq [accessed 2 May 2018]

သတင်းအချက်အလက်နည်းပညာနှင့်ဆိုက်ဘာလုံခြုံရေး ဦးစီးဌာန လက်ရှိ ဖွဲ့စည်းပုံ



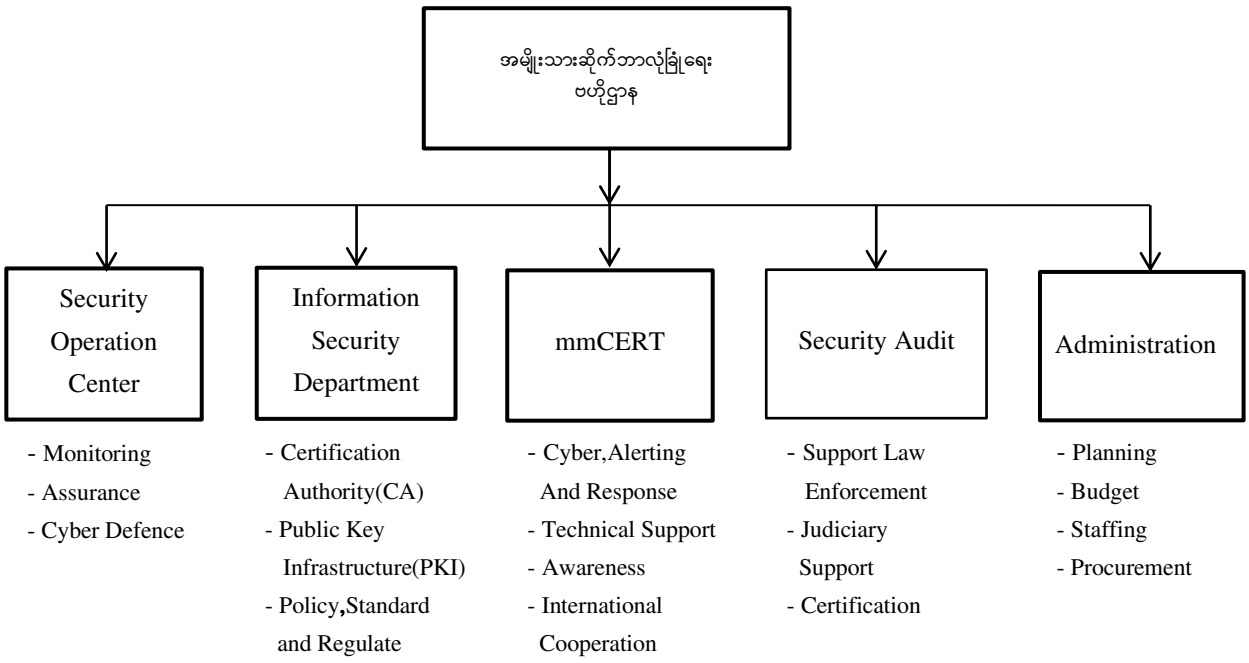
၁၃။ ပို့ဆောင်ရေးနှင့် ဆက်သွယ်ရေးဝန်ကြီးဌာနမှ ဆိုက်ဘာလုံခြုံရေးလုပ်ငန်းများ အကောင်အထည်ဖော်ဆောင်ရွက်နိုင်ရေးအတွက် ICT ကော်မတီအား နိုင်ငံတော်သမ္မတရုံး၏ တိုက်ရိုက်ကြီးကြပ်ကွပ်ကဲမှုဖြင့် အောက်ပါပုံအတိုင်း ဖွဲ့စည်းဆောင်ရွက်သင့်ကြောင်း Myanmar e-Governance Master Plan (2016-2020)တွင် ဖော်ပြထားပါသည်။ e-Government လုပ်ဆောင်ချက်အားလုံးကို နိုင်ငံတော်သမ္မတရုံးမှ တိုက်ရိုက်ကြီးကြပ်၍ အချိန်ကာလတစ်ခုတွင် ကော်မတီအား သင့်လျော်ရာ ဝန်ကြီးဌာန၏ ကြီးကြပ်မှုအောက်သို့ ပြောင်းရွှေ့သွားရန်ဖြစ်ပါသည်။

အဆိုပြု နိုင်ငံတော် သမ္မတရုံး၊အမျိုးသား ICT ကော်မရှင်/ကော်မတီ ဖွဲ့စည်းပုံ



၁၄။ အမျိုးသားဆိုက်ဘာလုံခြုံရေးဗဟိုဌာန၏လုပ်ငန်းတာဝန်များမှာ သတင်းအချက်အလက် လုံခြုံရေးဆိုင်ရာမူဝါဒ၊ လမ်းညွှန်ချက်များချမှတ်ခြင်း၊ ကြီးကြပ်ဆောင်ရွက်ခြင်း၊ အစိုးရသတင်း အချက်အလက်ကွန်ရက်အား စောင့်ကြည့်ခြင်း၊ ကာကွယ်ခြင်း၊ အရေးပေါ်ကိစ္စရပ်များအား တုန့်ပြန်ခြင်း၊ အသိပညာဖြန့်ဝေခြင်း၊ သတင်းအချက်အလက်နည်းပညာလုံခြုံရေး စစ်ဆေးပေး ခြင်း၊ ဆိုက်ဘာလုံခြုံရေး ကျိုးပေါက်မှုများအတွက် ပြည်တွင်း/ပြည်ပ အဖွဲ့အစည်းများနှင့် ပူးပေါင်း ဆောင်ရွက်ခြင်း၊ အင်တာနက်နှင့်ကွန်ရက်ဝန်ဆောင်မှုပေးသူများအား ကြီးကြပ်ခြင်း၊ သတင်း အချက်အလက် လုံခြုံရေးအသိအမှတ်ပြုလက်မှတ်များ ထုတ်ပေးခြင်း ၊ စီမံကိန်းလုပ်ငန်းများ အတွက် ဘတ်ဂျက်ရေးဆွဲခြင်း ၊ ပစ္စည်းဝယ်ယူခြင်း ၊ အုပ်ချုပ်မှုကိစ္စများဆောင်ရွက်ခြင်းနှင့် ICT ကော်မတီမှ အခါအားလျော်စွာပေးအပ်သည့်တာဝန်များအား ဆောင်ရွက်ခြင်းတို့ဖြစ်ပါသည်။

အဆိုပြု အမျိုးသားဆိုက်ဘာလုံခြုံရေးဗဟိုဌာန ဖွဲ့စည်းပုံ



မြန်မာနိုင်ငံတွင်လက်ရှိကျင့်သုံးနေသော ဆက်သွယ်ရေးနှင့် သတင်းအချက်အလက်နည်းပညာ ဆိုင်ရာ ဥပဒေများ

၁၅။ မြန်မာနိုင်ငံတွင် လက်ရှိကျင့်သုံးနေသော ဆက်သွယ်ရေးနှင့် သတင်းအချက်အလက် နည်းပညာဆိုင်ရာ ဥပဒေများမှာ ဖော်ပြပါအတိုင်း ဖြစ်ပါသည်-

(က) ကွန်ပျူတာပညာဖွံ့ဖြိုးတိုးတက်ရေးဥပဒေ၊ (၁၉၉၆)

(ခ) အီလက်ထရွန်းနစ်ဆက်သွယ်ရေးဥပဒေ၊(၂၀၀၄၊၂၀၁၄)

(ဂ) ဆက်သွယ်ရေးဥပဒေ၊(၂၀၁၃)

၁၆။ ပြဋ္ဌာန်းပြီးဥပဒေများတွင် ICT လုပ်ငန်းဖွံ့ဖြိုးတိုးတက်ရေး၊ အစိုးရအုပ်ချုပ်မှုယန္တရား တွင်ကွန်ပျူတာနည်းပညာအား အသုံးချရေးတို့အတွက် ပါဝင်သော်လည်း တည်ဆဲဥပဒေများတွင် e-Government စနစ်တိုးတက်လာစေရေးအတွက် အထောက်အကူပြုနိုင်မည့် အခြေခံအချက်များ မပါဝင်ကြောင်း တွေ့ရှိရပါသည်။[5]လက်ရှိတွင် Cyber Legal and Policy Framework (Cyber Law) ကိုရေးဆွဲနိုင်ရန် ကမ္ဘာဘဏ်ချေးငွေဖြင့် ဆောင်ရွက်လျက်ရှိပြီး ၂၀၁၉ ခုနှစ် အစောပိုင်းတွင် ဥပဒေမူကြမ်းရရှိရန် လျာထားဆောင်ရွက်လျက်ရှိပါသည်။[6]

ဆိုက်ဘာကျိုးပေါက်မှုအား ကာကွယ်ရန်နည်းလမ်းများ

၁၇။ ဆိုက်ဘာကျိုးပေါက်မှုဖြစ်ပေါ်လာလျှင် တိုက်ခိုက်ခံရသည့် အဖွဲ့အစည်းအနေဖြင့် နိုင်ငံ အတွင်း အဖွဲ့အစည်းပေါင်းစုံပါဝင်ဖွဲ့စည်းထားသော(Cyber Team) အဖွဲ့နှင့် ပူးပေါင်းဆောင်ရွက် ရန်အထူးလိုအပ်ပါသည်။ ပေါင်းစပ်ညှိနှိုင်းမှုမရှိသည့်အတွက် အဖွဲ့အစည်းများအနေဖြင့် အမြင့်မား ဆုံးသော ခြိမ်းခြောက်မှုများကို တုန့်ပြန်မှုနှင့် ကာကွယ်မှုများ မပြုလုပ်နိုင်ပါ။

၁၈။ ဆိုက်ဘာခြိမ်းခြောက်မှုခံရသည့်အဖွဲ့အစည်း (ဥပမာ- ဘဏ်၊ ဝန်ကြီးဌာန) စသည်တို့သည် လုံခြုံရေးဆိုင်ရာအဖွဲ့အစည်းများဖြင့် ပူးပေါင်းဆောင်ရွက်ရန်နှင့် ကြိုတင်ကာကွယ်ရန် စီမံခန့်ခွဲမှု စနစ်ရှိရန် လိုအပ်ပါသည်။ (ဥပမာ- IT ပညာရှင်ကို အခကြေးငွေပေး၍ ခန့်ထားခြင်း)

၁၉။ ပထမအချက်အနေဖြင့် လုံခြုံရေးအပိုင်းတွင် စွန့်စားခြင်းနှင့်အောင်မြင်မှုတန်ဖိုးကြားတွင် ခြားနားမှုများရှိပါသည်။ အိုင်တီကျွမ်းကျင်သူများမှာ စီးပွားရေးခေါင်းဆောင်များနှင့် ဆက်သွယ် ဆောင်ရွက်မှုများမရှိပါ။ အမှုဆောင်အရာရှိများကလည်း မဖြစ်သေးသည့် ဆိုက်ဘာတိုက်ခိုက်မှု များတွင် ရင်းနှီးမြှုပ်နှံမှုဆိုင်ရာ အလားအလာများနှင့် အခက်အခဲများ ရင်ဆိုင်ရလျက်ရှိပါသည်။ စီးပွားရေးခေါင်းဆောင်များမှာလည်း လုံခြုံရေးဆိုင်ရာ ကျိုးပေါက်မှုများတွင် ဖြစ်တတ်သော

---

[5] Available From: Myanmar e-Government Master Plan (2016-2020) Myanmar Version (Draft).pdf [accessed 4 May 2018]

[6] Available From: ၂၀၁၈ ခုနှစ်၊ မေလ ၁၀ ရက်နေ့ထုတ် မြန်မာ့အလင်းသတင်းစာ၊ စာမျက်နှာ ၇ မှ ကောက်နှုတ်ထားပါသည်။ (ကြည့်ရှုသည့်ရက် ၁၀-၅-၂၀၁၈)

စီးပွားရေးအပေါ်အကျိုးသက်ရောက်မှု၊ အသိဉာဏ်ဆိုင်ရာမူပိုင်ခွင့်များ၊ ဂုဏ်သိက္ခာဆိုင်ရာများနှင့် ပတ်သက်၍ သက်ရောက်မှုအနည်းအများကို နားလည်ထားသင့်ပါသည်။

၂၀။ အိုင်တီပညာရှင်များကလည်း ညှိနှိုင်းဆွေးနွေးပွဲများတွင် သက်ဆိုင်ရာအိုင်တီအကြောင်းအရာများကို စီးပွားရေးခေါင်းဆောင်များနားလည်အောင် ကြိုးစားလုပ်ဆောင်သင့်ပါသည်။ ထို့အတူ ဆိုက်ဘာလုံခြုံရေး ရင်းနှီးမြှုပ်နှံမှု၏ တန်ဖိုးကိုလည်း နားလည်သဘောပေါက်အောင် လုပ်ဆောင်ပေးရပါမည်။ စီးပွားရေးခေါင်းဆောင်များအနေဖြင့်လည်း ၎င်းတို့၏ အိုင်တီဌာနများကို လုံခြုံရေးဆိုင်ရာရည်မှန်းချက်များ အပြည့်အဝနားလည်အောင်လုပ်ဆောင်ရမည်ဖြစ်ပါသည်။

၂၁။ ဒုတိယအချက်အနေဖြင့် လုံခြုံရေးအဖွဲ့သည် အင်တာပရိုက်စ်တစ်ခုလုံးကို အချိန်တိုင်းကြည့်နေရန်လိုပါသည်။ လက်ရှိကမ္ဘာကြီးတွင် မိုဘိုင်းနည်းပညာ၊ ကလောက်နည်းပညာနှင့် အင်တာနက်နည်းပညာများမှာ ဆိုက်ဘာခြိမ်းခြောက်တိုက်ခိုက်မှုကို အချိန်တိုင်း လမ်းဖွင့်ပေးနေသကဲ့သို့ ဖြစ်နေပါသည်။ ဆိုက်ဘာခြိမ်းခြောက်မှုများမှာ ၃၉ စက္ကန့်တိုင်းတွင် တစ်ကြိမ်ဖြစ်ပေါ်လျက်ရှိသည့်အတွက် ဆိုက်ဘာနှင့် ဆက်စပ်သောလုံခြုံရေးကဏ္ဍ/အဖွဲ့များ စဉ်ဆက်မပြတ်လေ့လာစောင့်ကြည့်မှုသည် စနစ်တကျရှိရန်လိုအပ်ပါသည်။တတိယအချက်မှာ တင်ပြပါလုံခြုံရေးအဖွဲ့ကို ဆိုက်ဘာတိုက်ခိုက်လာမှုမှကာကွယ်ရန်နှင့် ခြိမ်းခြောက်မှုမှတန်ပြန်လုပ်ဆောင် နိုင်ရန်အတွက် လုပ်ပိုင်ခွင့်များ အပြည့်အဝပေးထားရန်ဖြစ်ပါသည်။ ဆိုက်ဘာခြိမ်းခြောက်မှု ဖြစ်ပေါ်လာလျှင် အလျင်အမြန်တုံ့ပြန်မှုသို့မဟုတ် နည်းပညာလိုအပ်ချက် (၇၄ ရာခိုင်နှုန်း) ၊ ပြန်လည်တုံ့ပြန်ရန် နှောင့်နှေးမကျေနပ်မှု (၉၀ ရာခိုင်နှုန်း) ရှိကြောင်း လေ့လာတွေ့ရှိရပါသည်။[7]

အကြီးမားဆုံးသော ဆိုက်ဘာလုံခြုံရေး ခြိမ်းခြောက်မှု (၅)မျိုး

၂၂။ ၂၀၁၇ ခုနှစ် တစ်နှစ်လုံး ဆိုက်ဘာတိုက်ခိုက်မှု အများအပြားဖြစ်ပေါ်ခဲ့ပါသည်။ ၎င်းတို့အနက် မြောက်ကိုရီးယားနိုင်ငံမှ ကမ္ဘာအနှံ့အပြားရှိ ကွန်ပျူတာအလုံးပေါင်း ၂၅၀,၀၀၀ ကျော်ကို Wanna Cry ဖြင့်တိုက်ခိုက်မှုမှာလည်း တစ်ခုအပါအဝင်ဖြစ်ပါသည်။ NotPetya Cyber တိုက်ခိုက်မှုသည် ယူကရိန်းနှင့်ရုရှားမှ ကုမ္ပဏီလုပ်ငန်းများကိုထိခိုက်ခဲ့ပြီး အမေရိကန်နိုင်ငံသား ၁၄၃ သန်း၏ သတင်းအချက်အလက်များကို ထိခိုက်ခဲ့သည်။ အမေရိကန်နိုင်ငံရှိ သုတေသနနှင့်နည်းပညာကုမ္ပဏီ

[7] ဆိုက်ဘာကျိုးပေါက်မှုတွေမဖြစ်အောင် ဘယ်လိုကာကွယ်မလဲ၊ တင်လင်းအောင်၊ ၂၀၁၈ ခုနှစ်၊ ဧပြီလ ၁၂ ရက်နေ့ထုတ် မြန်မာ့အလင်းသတင်းစာ၊ စာမျက်နှာ ၁၅ မှ ကောက်နှုတ်ထားပါသည်။ (ကြည့်ရှုသည့်ရက် ၁၂-၄-၂၀၁၈)

Gartner အရ ၂၀၁၇ ခုနှစ်တွင် နည်းပညာလုံခြုံရေးအတွက် အသုံးပြုငွေ အမေရိကန်ဒေါ်လာ ၈၆.၄ ဘီလီယံအထိရှိခဲ့ပါသည်။ ၂၀၁၈ ခုနှစ်တွင်လည်း အမေရိကန်ဒေါ်လာ ၁၁၀ ဘီလီယံအထိ အသုံးပြုမည်ဟု ခန့်မှန်းထားပါသည်။ ဆိုက်ဘာလုံခြုံရေးအဖွဲ့မှ ၂၀၁၈ ခုနှစ်တွင် ဖြစ်ပေါ်နိုင်သော ဆိုက်ဘာခြိမ်းခြောက်မှု အကြီးမားဆုံး (၅)ခုမှာ -

(က) **ဟတ်ကာများ၏ ပစ်မှတ်ဖြစ်လာသော ဒစ်ဂျစ်တယ်ငွေကြေးစနစ်။** ၂၀၁၈ ခုနှစ်တွင် အမေရိကန်ငွေကြေးသည် ဟတ်ကာများကြောင့် ပစ်မှတ်ဖြစ်လာပါသည်။ ၎င်းကို Cryptojacking ဟုခေါ်ပါသည်။ နောင်ကာလတွင် ကုမ္ပဏီများ၊ တစ်ဦးချင်း သို့မဟုတ် အုပ်စုများ၏ ကုန်သွယ်မှုနှင့် ဒစ်ဂျစ်တယ်ငွေကြေးစနစ်များသည် ဟတ်ကာများ၏ ပစ်မှတ်ဖြစ်လာပါသည်။

(ခ) **ဆိုက်ဘာတိုက်ခိုက်မှုအခြေခံ၍ တစ်ဟုန်ထိုးတိုးတက်လာသော စွမ်းအား။** ဆော်ဒီအာရေဗျကုမ္ပဏီများရှိ ကြီးကြပ်ထိန်းချုပ်မှု Server များတွင် သူလျှို အဖျက်အမှောင့်များထား၍ သတင်းအချက်အလက်ခိုးယူမှုများ အစပျိုးလာနိုင်ပါသည်။

(ဂ) **အစိုးရကြီးမှူးသော ဆိုက်ဘာပြစ်မှုများ။** မြောက်ကိုရီးယား၊ ရုရှား၊ တရုတ်တို့တွင် အစိုးရထောက်ကူကြီးကြပ်မှုဖြင့် အဆက်မပြတ်ဆိုက်ဘာတိုက်ခိုက်မှုများ ရှိလာနိုင်ပါသည်။ (ဥပမာ - မြောက်ကိုရီးယား၏ လာဇာရပ်စ်ဆိုက်ဘာအုပ်စု)

(ဃ) **လုံခြုံရေး ဆော်ဖ်ဝဲလ် များကို ထိုးဖောက်လာမည့် အဓိကအချက်။** ၂၀၁၈ ခုနှစ်တွင် ယုံကြည်စိတ်ချရသော Program များ၊ Software များ၊ Hardware များကို ထုတ်လုပ်ဖြန့်ဖြူးသည့် လုံခြုံရေး Software ကုမ္ပဏီများကို ပစ်မှတ်ထားတိုက်ခိုက်မှုများရှိလာနိုင်ပါသည်။

(င) **ကွန်ပျူတာကို ပျက်ဆီးစေသော Worms ။** ပစ်မှတ်ကို အလျင်အမြန် ဖျက်ဆီးတိုက်ခိုက်နိုင်သည့် Malware မျိုးကွဲ Worms များ အများအပြားအသုံးပြုတိုက်ခိုက်လာနိုင်ပါသည်။[8]

[8] Available From: https://www.cybersecurity-insiders.com/top-5-cybersecurity-threats-of-2018/[accessed 7 May 2018]

ဆိုက်ဘာတိုက်ခိုက်ခံရမှုများအား နားလည်စေနိုင်သည့် ဆိုက်ဘာလုံခြုံရေး အချက် (၂၀)

၂၃။ ကွန်ပျူတာ၊ အင်တာနက် သုံးစွဲသူများအနေဖြင့် သိသာသောဆိုက်ဘာတိုက်ခိုက်မှုများနှင့် ကြုံတွေ့နိုင်သကဲ့သို့ တစ်ခါတစ်ရံ မသိနိုင်သောတိုက်ခိုက်မှုများနှင့်လည်း ကြုံတွေ့ရနိုင်ပါသည်။ အောက်ပါအချက်များသည် ဆိုက်ဘာတိုက်ခိုက်ခံရမှုအား နားလည်စေနိုင်သော အချက်များဖြစ်ပါသည်-

(က) **ထူးခြားသောလက္ခဏာများ** ။ ဗိုင်းရပ်စ်များ ကူးစက်စေခြင်း၊ဝက်ဘ်ဆိုက်များအား တရားမဝင် ဝင်ရောက်အသုံးပြု၍ အရေးကြီးသော အချက်အလက်များအား အလွဲသုံးစားပြုလုပ်ပြီး လူမှုရေးနှင့်နိုင်ငံရေး ပြဿနာများ ဖြစ်ပေါ်စေရန် ရည်ရွယ်တိုက်ခိုက်မှုဖြစ်ပါသည်။နောက်ဆက်တွဲဆိုးကျိုးအနေဖြင့် သက်သေခံအချက်အလက်ခိုးယူခြင်း၊ ခြိမ်းခြောက်ခြင်း၊ ဖန်တီးမှု မူပိုင်ခွင့်များခိုးယူခြင်း၊ စက်ပစ္စည်းများနှင့် အချက်အလက်များ အသုံးပြုခွင့်ဆုံးရှုံးခြင်း၊ ဝက်ဘ်ဆိုက်မျက်နှာစာများ ဖျက်စီးခြင်းစသည့် ဆိုးကျိုးများဖြစ်ပေါ်လာပါသည်။

(ခ) **နိုင်ငံသားတစ်ဦး၏ဆိုက်ဘာလုံခြုံရေးနှင့် တာဝန်ကြားဆက်သွယ်မှု။** နိုင်ငံသားတစ်ဦးအနေဖြင့် ဆိုက်ဘာနယ်ပယ်လုံခြုံမှုရှိစေရန်နှင့် စောင့်ထိန်းလိုက်နာရန်နည်းပညာအသုံးချမှုများကိုအသုံးပြုနိုင်ရမည်။ သက်ဆိုင်သောစည်းမျဉ်း၊ စည်းကမ်း၊ ထုံးတမ်းများကိုသိရှိခြင်း၊ ဗဟုသုတများဝေမျှခြင်း၊ အွန်လိုင်းကိုယ်ပိုင်လွတ်လပ်ခွင့်ထိန်းသိမ်းခြင်း၊ မူပိုင်ခွင့်မူဝါဒများအား အလေးထားခြင်း၊ ဖျက်ဆီးရေးလှုပ်ရှားမှုများအားတားဆီးရန် ကိုယ်ထူကိုယ်ထကင်းချခြင်းနှင့် အကင်းပါးစွာလှုပ်ရှားခြင်းများအားဖြင့် လူတိုင်းက အင်တာနက်ကို ပိုမိုကောင်းမွန်သောနေရာ ဖြစ်လာစေရန် ဆောင်ရွက်နိုင်ကြပါသည်။ ထိုထက်ပိုပြီး နိုင်ငံသားများက အွန်လိုင်းပေါ်တွင် မည်သူမည်ဝါ လွယ်ကူစွာမသိနိုင်ခြင်းအပေါ်တွင်လည်း အခွင့်ကောင်းမယူသင့်ပါဟု ယူဆပါသည်။

(ဂ) **အင်တာနက်အား အသုံးချခြင်း** ။ အင်တာနက်ကွန်ရက်၏အကျယ်အဝန်းသည် လွန်ခဲ့သည့်ဆယ်စုနှစ်တစ်စုကျော်စာ အတွေ့အကြုံများဖြင့် များစွာတိုးတက်

ပြောင်းလဲလာပြီး Local Area Network (LAN) နှင့် Wide Area Network (WAN)တို့ပေါင်းစပ်ခြင်းသည်လည်းကွန်ရက်တစ်ခုတည်းအဖြစ် အသုံးပြုနိုင်သည့် စပ်ကြောင်းမဲ့ကွန်ရက် (SeamlessNetwork) တစ်ခုကို ဖန်တီးပေးခဲ့ပါသည်။ ထိုကဲ့သို့ကြီးမားသော ဆက်သွယ်မှုများတွင် ဗဟိုအုပ်ချုပ်ရေးစနစ်များ ကင်းမဲ့နေတတ်ကြပါသည်။ ကမ္ဘာ့လူဦးရေ၏ ၅၀ ရာခိုင်နှုန်းခန့်သည် အင်တာနက်အသုံးပြုနေကြပြီး ၎င်းတို့၏ ၄၂ရာခိုင်နှုန်းခန့်က အွန်လိုင်းအရောင်းအဝယ်များ လုပ်ကြပါသည်။ ထိုကဲ့သို့ ဆက်သွယ်မှုများကြားတွင် ကမ္ဘာ့တစ်ဖက်ခြမ်းမှပြဿနာတစ်ခုက အခြားတစ်ဖက်ခြမ်းသို့ ချက်ချင်း ပျံ့နှံ့ကူးစက်သွားရန် လွယ်ကူပါသည်။ ထို့ပြင် Transmission Control Protocol (TCP) သို့မဟုတ် Internet Protocol တို့ကို အလွယ်တကူ စုစည်းထားခြင်းနှင့်အတူ အလွန်ဆိုးဝါးရှုပ်ထွေးသော ကွန်ပျူတာကွန်ရက်စီမံခန့်ခွဲရေး စနစ်များသည်လည်း ဆိုက်ဘာတိုက်ခိုက်ခံရမှုများကို ဖြစ်ပေါ်စေပါသည်။

(ဃ) **Hackingtool များအလွယ်တကူရခြင်း။** Hackingtoolများ အလွယ်တကူရနိုင်ခြင်းသည်လည်း ဆိုက်ဘာဒုစရိုက်မှုများဖြစ်စေရန် အားပေးအားမြှောက် ပြုနေပါသည်။ ဂိမ်းနှင့် Hacking ဖိုရမ်များပေါ်တွင် များစွာသော တရားမဝင် Hacking အထောက်အကူပြုပစ္စည်းများကို အဆင်သင့်ရနိုင်ပြီ ဖြစ်ပါသည်။ DDOS နှင့် Ransomware များကဲ့သို့ Hacking Tool များကိုတစ်ဆင့်ချင်း ရှင်းလင်းထားသော သင်ခန်းစာများနှင့်အတူ လူတိုင်းလက်လှမ်းမှီသောဈေးနှုန်းဖြင့် အလွယ်တကူရနိုင်ခြင်းက မည်သူ့ကိုမဆို တရားဝင်ဝက်ဘ်ဆိုက်တစ်ခုခုကို ရယူစေနိုင်ပါသည်။ ၎င်းဖော်ပြချက်များသည် ငယ်ရွယ်သူများကို ဆိုက်ဘာဒုစရိုက်မှုများတွင် ပါဝင်စေရန် ပို၍တွန်းအားပေးနေပါသည်။

(င) **ဆိုက်ဘာတိုက်ခိုက်မှုများကြောင့် ရရှိနိုင်သော အဆုံးအစမဲ့ ဆိုးကျိုးများ။** ရုတ်တရက် မှောင်ပိတ်သွားခြင်း၊ အဏုမြူစက်ရုံများပုံမှန်မလည်ပတ်ခြင်း၊ ပိုက်လိုင်းများ ပေါက်ကွဲခြင်း၊ မီးရထားနှင့်လေကြောင်းလိုင်းများ၏ ခရီးစဉ်ဖော်ပြချက်များ

ကမောက်ကမဖြစ်ခြင်း၊ သက်သေခံအချက်များခိုးယူခြင်း၊ အွန်လိုင်းလုပ်ငန်းအသွား အလာများမှားယွင်းခြင်းနှင့် ဝက်ဘ်ဆိုက်များ သိမ်းပိုက်ခံရခြင်း စသည်တို့သည် ဆိုက်ဘာတိုက်ခိုက်မှု၏ နောက်ဆက်တွဲရလဒ်များ ဖြစ်ပါသည်။ ဂိမ်းကုမ္ပဏီများ၊ ဘဏ္ဍာရေးလုပ်ငန်းအဖွဲ့များ၊ အီလက်ထရောနစ် စီးပွားရေးလုပ်ငန်းများ၊ လူမှုကွန်ယက်များနှင့် ဒေတာစင်တာများသည် ဟက်ကာများအတွက် အကျိုးအမြတ်များသော ပစ်မှတ်များဖြစ်နေပါသည်။ ကမ္ဘာ့နိုင်ငံအသီးသီးကလည်း ၎င်းသတင်းအချက်အလက်တိုက်ခိုက်မှုပြဿနာအား ကိုင်တွယ်ဖြေရှင်းလျက်ရှိပါသည်။

(စ) **ကမ္ဘာ့ဟက်ကာလှုပ်ရှားမှုအတက်ကြွဆုံးနိုင်ငံများ။** Internet Solution မှ ၂၀၁၆ ခုနှစ်၏ Global Threat Intelligence မှတ်တမ်း ထုတ်ပြန်ချက်အရ တိုက်ခိုက်မှုများ၏ (၆၅) ရာခိုင်နှုန်းသည် အမေရိကန်ပြည်ထောင်စုနှင့် မြေပြင်တည်နေရာ ပိတ်ဆို့ခြင်းများကို ရှောင်ရှားရန် အသုံးပြုသည့် ဟက်ကာများလွှမ်းမိုးထားသော Host များ၏ IP များမှ စတင်ခဲ့ပါသည်။ တရုတ်နိုင်ငံသည် Hacking လှုပ်ရှားမှုရှိသော နိုင်ငံများစာရင်း၏ထိပ်ဆုံးနေရာတွင် ကမ္ဘာ့ Hacking လှုပ်ရှားမှုများ၏ ၄၁ ရာခိုင်နှုန်းဖြင့် ရပ်တည်နေဆဲပင်ဖြစ်ပါသည်။ တရုတ်နိုင်ငံ၏ Hacking အတွက် ဦးဆောင်မှုများကို ဆိုက်ဘာလုံခြုံရေးနှင့် တရုတ်နိုင်ငံတက္ကသိုလ်များမှ ကျင်းပသော Hacking ပြိုင်ပွဲများအား တရားဝင်အထောက်အပံ့ပေးနေသည့် တရုတ်နိုင်ငံအစိုးရ၏ အစိတ်အပိုင်းတစ်ခုအဖြစ် ယူဆနိုင်ပါသည်။ တရုတ်၊ အမေရိကန်၊ တူရကီနှင့် ရုရှားနိုင်ငံများသည် ဆိုက်ဘာတိုက်ခိုက်မှုဖြစ်စဉ်များ၏ (၆၀)ရာခိုင်နှုန်း အထက်တွင် တာဝန်ရှိပါသည်။

(ဆ) **အမြဲတမ်းလူသိအများဆုံး Hacking အဖွဲ့များ ။** Lizard Squad အဖွဲ့သည် Facebook၊ မလေးရှားလေကြောင်းလိုင်း ဝက်ဘ်ဆိုက်၊ Microsoft Xbox Live နှင့် Sony ၏ Playstation ကွန်ရက်များကို Hackခဲ့ပါသည်။ Anonymous အဖွဲ့တွင် ထောင်ပေါင်းများစွာသော Hacktivists များ ပါဝင်ပြီး ၎င်း၏ပစ်မှတ် များမှာ Master Card, Visa, PayPal နဲ့ NewYork မြို့၏စတော့လဲလှယ်ခြင်း

ဝက်ဘ်ဆိုက်ဒ်များဖြစ်ပါသည်။ Chaos Computer Club (CCC)အဖွဲ့သည် ဂျာမဏီနိုင်ငံတွင် ၁၉၈၁ ခုနှစ်အတွင်း၌ဖွဲ့စည်းခဲ့ပြီး ရှေးအကျဆုံး၊ ဝါအရင့်ဆုံး ကျင့်ဝတ်လိုက်နာသော ဟက်ကာအဖွဲ့လည်း ဖြစ်ပါသည်။ ၎င်းတို့၏ ရည်ရွယ်ချက်မှာ အဓိကကျသည့်စနစ်များတွင်ဖြစ်နေသော လုံခြုံရေးယိုပေါက်များကို ရှာဖွေရန် ဖြစ်ပါသည်။ OurMine အဖွဲ့သည် Mark Zuckerberg နှင့် Sundar Pichai တို့၏ လူမှုကွန်ယက် အကောင့်များကို Hack ခဲ့ကြပါသည်။ ထို့အပြင်၎င်းတို့သည် LinkedIn ကိုလည်း တိုက်ခိုက်ခဲ့ပါသည်။ ၎င်းအဖွဲ့က ဆိုက်ဘာတိုက်ခိုက်မှုများအပြင်ဆိုက်ဘာလုံခြုံရေးစစ်ဆေးခြင်းဝန်ဆောင်မှုများလည်းပေးကြပါသည်။ အခြားထင်ရှားသည့်အဖွဲ့များမှာ LulzSec၊ Syran Electronic Army၊ The Level Seven Crew၊ globalHell နှင့် Tea Mp0isoN တို့ဖြစ်ပါသည်။

(ခ) **ဆိုက်ဘာပျော့ကွက်များနှင့်ပတ်သက်၍ နားလည်နိုင်ရန် အရေးကြီးသောအချက်များ** ။ Adobe Reader၊ Flash Player များကဲ့သို့ Java အခြေပြု ပရိုဂရမ်များကို ကွန်ပျူတာအများစုတွင် အသုံးပြုနေပါသည်။ ထို့ပြင် ၎င်းပရိုဂရမ်များက ဗိုင်းရပ်စ်၊ Worm နှင့် Trojan Horse များပါဝင်သော ဖျက်ဆီးရေးဆော့ဖ်ဝဲလ် များဖြင့် တိုက်ခိုက်သည့် ရိုးရှင်းသော Syntactic Attack ဟုခေါ်သည့် တိုက်ခိုက်မှုကိုခုခံနိုင်ရန်လွန်စွာအားနည်းကြပါသည်။ ထို့ကြောင့် ကွန်ပျူတာအများစုတွင် ဆော့ဖ်ဝဲလ် ပျော့ကွက်များရှိနေပါသည်။ ကမ္ဘာအနှံ့အပြားမှ အစိုးရအဖွဲ့အစည်းများသည် ၎င်းတို့၏ (အခြားအစိုးရတစ်ခုကို ယှဉ်၍စစ်ရေးစစ်ရာ (သို့မဟုတ်) နိုင်ငံရေးအရ အရေးသာမှုရရန် Hackingများ ပြုလုပ်ခြင်း) သူလျှိုစစ်ဆင်ရေးများအတွက် ဖျက်ဆီးရေးပရိုဂရမ်များ၊ ဖွံ့ဖြိုးတိုးတက်မှုစစ်ဆင်ရေးများတွင် အကြွင်းမဲ့ပါဝင် ထောက်ပံ့ပေးကြပါသည်။ Stuxnet မှာ ထိုကဲ့သို့ ဖျက်ဆီးရေးပရိုဂရမ်များအတွက် အကောင်းဆုံးဥပမာတစ်ခုပင်ဖြစ်သည်။

(ဈ) **အခြေခံဆိုက်ဘာဒုစရိုက်မှုပုံစံများအား အတိုချုပ်အားဖြင့် ဖော်ပြခြင်း** ။ ဆိုက်ဘာ ဒုစရိုက်သမားများသည် နည်းလမ်းပေါင်းစုံဖြင့် အသုံးပြုတိုက်ခိုက်ကြပါသည်။ အသုံးများသောနည်းလမ်းအချို့မှာ -

(၁) **Hacking**။ ဟက်ကာများကနည်းလမ်းပေါင်းစုံအသုံးပြုပြီး ၎င်းတို့ပစ်မှတ်၏ကွန်ပျူတာများ၊ ကွန်ရက်များကို တရားမဝင်ဝင်ရောက်ရန် ကြိုးစား၍ Hack ခံရသည့် Device ကို လွှဲမှားစွာ အသုံးပြုရန်၊ ပိတ်ပစ်ရန် ဖြစ်ပါသည်။

(၂) **Cyber Stalking**။ ပစ်မှတ်အား စောင်ကားပုတ်ခတ် တိုက်ခိုက်သည့် အွန်လိုင်းပေးစာများဖြင့် နှောင့်ယှက်မှုဖြစ်ပါသည်။

(၃) **Identity Theft** ။ ဆိုက်ဘာရာဇဝတ်မှု ကျူးလွန်မည့်သူ တစ်ယောက်က ပြည်သူ၏ဘဏ်အကောင့်၊ ကြိုသုံးကဒ်နှင့် အခြားဘဏ္ဍာရေး အချက်အလက်များကို ဝင်ရောက်အသုံးပြုခွင့်ရယူ၍ ပိုက်ဆံခိုးခြင်း၊ မှောင်ခိုဈေးကွက်များတွင် ပြန်ရောင်းချရန် အွန်လိုင်းမှဈေးကြီးပစ္စည်းများကို ဝယ်ယူခြင်းများ ပြုလုပ်ကြပါသည်။

(၄) **Child Soliciting and Abuse** ။ ရာဇဝတ်သားများသည်ChatRoom မှတဆင့်လူငယ်များဆီမှ ကလေးသူငယ်အပြာပုံများ ရယူနိုင်ရန် ရည်ရွယ်၍ နည်းအမျိုးမျိုးဖြင့် ကြိုးစားရယူခြင်း ဖြစ်ပါသည်။

(ည) **ဆိုက်ဘာတိုက်ခိုက်သူများကို ရှုထောင့်အမျိုးမျိုးဖြင့် အမျိုးအစားခွဲခြားခြင်း** ။ မကျေမနပ်ဖြစ်နေသည့် ဝန်ထမ်းအဖွဲ့အစည်းမှ အတွင်းလူ၊ ငွေမက်သော ဝန်ထမ်းအတွင်းလူနှင့် အဖွဲ့ဟောင်းတွင်ပါဝင်ရင်း မတော်တဆ အတွင်းလူဖြစ်နေသူများစသည်ဖြင့် ဆိုက်ဘာတိုက်ခိုက်ရေးသမားများကို အတွင်းလူနှင့် အပြင်လူဟူ၍ အမျိုးအစားခွဲခြားနိုင်ပါသည်။မကျေမနပ်ဖြစ်နေသောဝန်ထမ်းများက အတွင်းပိုင်းစနစ်များ၏လုံခြုံရေးကို ခြိမ်းခြောက်မှုများပြုနိုင်ပါသည်။ ထိုနေရာတွင် ပိုက်ဆံမက်သော အတွင်းလူများသည် ကုမ္ပဏီ၏ပိုင်ဆိုင်မှုများကို ကိုယ်ကျိုးအတွက်အလွဲသုံးစားပြုနိုင်ပါသည်။ မတော်တဆအားဖြင့်လည်း အတွင်းလူဖြစ်နေသူများသည် ၎င်းတို့

ကိုယ်တိုင် မသိလိုက်ဘဲ၊ မရည်ရွယ်ဘဲလျှို့ဝှက်ချက်များ ပေါက်ကြားစေနိုင်ပါသည်။ အပြင်လူများကိုမူ အကြမ်းဖက်သမားများ၊ နိုင်ငံများနှင့်ဒုစရိုက်သမားများ ပေါင်းစုဖွဲ့စည်းထားသည့် တိုက်ခိုက်သူအဖွဲ့များအနေဖြင့် သိရှိနိုင်ပါသည်။

(ဌ) ဆိုက်ဘာတိုက်ခိုက်မှု အမျိုးမျိုးနှင့် ၎င်းတို့ကိုစတင်ရန် နည်းလမ်းများ ။

ဆိုက်ဘာတိုက်ခိုက်မှုများကို Syntactic တိုက်ခိုက်မှုနှင့် Sematic တိုက်ခိုက်မှုဟူ၍ ခွဲခြားနိုင်ပါသည်။ ဥပမာ - ဗိုင်းရပ်စ်၊ Worm နှင့် ထရိုဂျန်များကဲ့သို့ အဖျက်အမှောင့်ဆော့ဖ်ဝဲလ်များအသုံးပြု၍ တိုက်ခိုက်ခြင်းကို Syntactic တိုက်ခိုက်မှုဟုသိနိုင်ပါသည်။ ဗိုင်းရပ်စ်များက ကိုယ့်ကိုယ်ကိုပွားယူနိုင်ပြီး ၎င်းတို့၏ကုဒ်များကို စတင်အလုပ်လုပ်စေရန် မည်သည့်ဖိုင်များကိုမဆို ကူးစက်နိုင်ပါသည်။ Worm များကမူ အခြားဖိုင်များကိုမကူးစက်ဘဲ ကိုယ့်ကိုယ်ကို ထိန်းကြောင်းရပ်တည်နိုင်ပြီး၊ ကွန်ယက်အတွင်းသို့ မိမိကိုယ်ကို ပွားယူပုံနှံနိုင်ပါသည်။ ထိုကဲ့သို့ ဆော့ဖ်ဝဲလ်များသည် ၎င်းတို့လုပ်ငန်းပြီးမြောက်စေရန် စနစ်တစ်ခု၏ အရေးကြီးသောအားနည်းချက်များကိုတိုက်ခိုက်ကြပြီး ပိုမိုထိရောက်စေရန် ထရိုဂျန်များက ပစ်မှတ်၏ အချက်အလက်များ ရယူပေးကြပါသည်။ Semantic တိုက်ခိုက်မှုဆိုသည်မှာ တိုက်ခိုက်သူတစ်ဦးက ပစ်မှတ်အားလှည့်စားရန် ကွန်ရက်တစ်ခု (သို့မဟုတ်) စက်ပစ္စည်းတစ်ခုခုကို အသုံးချခြင်းဖြစ်ပါသည်။ အရေးကြီးသော အားနည်းချက်များကိုတိုက်ခိုက်ကြပြီး ပိုမိုထိရောက်စေရန် ထရိုဂျန်အသုံးပြုသူများကို လျှို့ဝှက်ချက်များအား ကိုယ်တိုင်ဖော်ထုတ်စေရန် လှည့်စားတိုက်ခိုက်ခြင်းဖြစ်ပြီး လွန်စွာပြင်းထန်သော တိုက်ခိုက်မှုများဖြစ်ပါသည်။ စတော့ခ်များကို ဈေးပေါပေါဖြင့် ရောင်းထုတ်စေရန်၊ စတော့ခ်ဈေးနှုန်းများအား ဟန်ဆောင်၍ ဖောင်းပွမှု ဖြစ်စေခြင်းကဲ့သို့ "Pump and Dump" လိမ်လည်တိုက်ခိုက်မှုများနှင့် အချက်အလက်ကောင်းများရယူရန် အသုံးပြုသောPhishing တိုက်ခိုက်မှုများသည် Semantic တိုက်ခိုက်မှု၏ ဥပမာများ ဖြစ်ပါသည်။

(၄) **အန္တရာယ်ကင်းစွာ အသုံးပြုနိုင်ရေးအတွက် သတိပြုရှောင်ရှားရန် ဆိုက်ဘာ ပြစ်မှုများ။**

(၁) **တစ်ခုခုအား Download လုပ်စေချင်သောကြောင့် စစ်တမ်းများ ဖြည့်ပေး ရန်တွန်းအားပေးခြင်း။** လိမ်လည်မှုစစ်တမ်းများ၊ ကြိုးသုံးကတ် အချက် အလက်များ၊နာမည်၊ အသက်စသော တောင်းခံခြင်းများကဲ့သို့ အချက်အလက် များ စုစည်းရယူခြင်းစသည်တို့ ဖြစ်ပါသည်။ ထိုကဲ့သို့တိုက်ခိုက်ခြင်းများအား ရှောင်ရှားနိုင်ရန်၊ ဆော့ဖ်ဝဲလ်တစ်ခုခု Download ရယူရန် Google Search မှတဆင့်သွားခြင်းထက် စိတ်ချရသောဝက်ဘ်ဆိုက်သို့ တိုက်ရိုက်သွားရောက် Download ရယူခြင်းများ ပြုလုပ်သင့်ပါသည်။

(၂) **အရန်ဘက်ထရီအချိန်တိုးလွန်းခြင်း။** အကယ်၍ စမတ်ဖုန်းအသုံးပြုသူ တစ်ယောက်က ၎င်း၏အရန်ဘက်ထရီအချိန်သည် ပုံမှန်မဟုတ်ဘဲ တိုးလွန်း ခြင်းတစ်ခုခုကို သတိပြုမိလျှင် ဘက်ထရီသုံးလွန်းသော ပရိုဂရမ်များအား ရှာဖွေထုတ်ပစ်ပြီး အခြေအနေထူး၊ မထူးကို ဆန်းစစ် ကြည့်သင့်ပါသည်။ အကယ်၍ ဘက်ထရီအချိန်တိုးလာလျှင် အဖျက်အမှောင့်ပရိုဂရမ်တိုက်ခိုက်မှု ဖြစ်နိုင်ခြေရှိသည်ဟု ယူဆနိုင်ပါသည်။

(၃) **ဆိုက်ဘာတိုက်ခိုက်မှုဖြစ်ပွားခါနီး ရှေ့ပြေးလက္ခဏာများ ။** ဆိုက်ဘာတိုက်ခိုက် မှုတစ်ခု၏ ရှေ့ပြေးလက္ခဏာအများစုသည် ပထမပိုင်းတွင် အန္တရာယ်မရှိနိုင်ဟုယူဆ ရသော်လည်းစက်ပစ္စည်းများခေတ်နောက်ကျနေခြင်းသို့မဟုတ် အခြေခံအစိတ်အပိုင်း တစ်ခုခုဖြစ်ခြင်းကဲ့သို့ ထင်ရပါသည်။ အောက်တွင်ဖော်ပြထားသော အချက်ပြခြင်း များအား သတိပြုမိလျှင် တိုက်ခိုက်ခြင်းအား အချိန်မှီ တားဆီးနိုင်ပါလိမ့်မည်-

(၁) **အင်တာနက်နှေးကွေးသွားခြင်း။** အင်တာနက်ချိတ်ဆက်မှု နှေးကွေး သွားခြင်းသည်လည်း ဆိုက်ဘာတိုက်ခိုက်ခြင်း လက္ခဏာတစ်ခု ဖြစ်နိုင် ပါသည်။ ဝန်ဆောင်မှုများ ရပ်တန့်သွားစေရန် တိုက်ခိုက်ခြင်း (DOS) နှင့် ဝန်ဆောင်မှုများ ရပ်တန့်သွားစေရန် ဖြန့်ကျက်တိုက်ခိုက်ခြင်း Distributed

Denial of Service (DDOS) တိုက်ခိုက်မှုများသည် အင်တာနက်ချိတ်ဆက်မှု နှေးကွေးသွားခြင်းများ ဖြစ်စေနိုင်ပါသည်။

(၂) **Antivirus အသိပေးစာတုများ။** ပုံမှန်ကာကွယ်ထားခြင်း မရှိသော ကွန်ပျူတာများတွင် သတိပေးစာတုများဖြစ်ပေါ်နိုင်ပြီး ၎င်းစာများက အသုံးပြုသူကို Antivirus ပရိုဂရမ်ဟုထင်ရသော ပရိုဂရမ်တစ်ခုခုကို Install လုပ်ခိုင်းပါလိမ့်မည်။

(၃) **မလိုအပ်သော Browser Toolbar များပေါ်ခြင်း။** အကယ်၍ အသုံးပြုသူသည် Install မလုပ်ထားသော Browser toolbar တစ်ခုခုအား သတိပြုမိပြီဆိုလျှင် Browsing လုပ်နေချိန်တွင် ၎င်းကိုအခြားဝက်ဘ်ဆိုက်တစ်ခုခုဆီသို့ ခေါ်သွားလား၊ မခေါ်သွားလားဆိုသည်ကို သတိပြုစစ်ဆေးသင့်ပါသည်။ အကယ်၍ အခြားဝက်ဘ်ဆိုက်တစ်ခုခုဆီသို့ ခေါ်သွားသည်ဆိုလျှင် ဆိုက်ဘာ တိုက်ခိုက်ခံရခြင်း ဖြစ်နိုင်ပါသည်။

(ဃ) **စနစ်တစ်ခုသိမ်းပိုက်ခံလိုက်ရသည်ကို သေချာစေသောလက္ခဏာများ**

(၁) **ပုံမှန်မဟုတ်သော ဝက်ဘ်ကင်မရာ လုပ်ဆောင်မှုများ။** အကယ်၍ အသုံးပြုသူ၏ကွန်ပျူတာ ဝက်ဘ်ကင်မရာ၏မီးသည် အလိုအလျောက် ပိတ်/ဖွင့်လုပ်နေလျှင်ပေါ်ပြူလာဖြစ်သော အဖျက်အမှောင့်ပရိုဂရမ်တစ်ခုဖြစ်သည့် အဝေးမှထိန်းချုပ်ခြင်းပရိုဂရမ် ကူးစက်မှုခံနေရခြင်း ဖြစ်နိုင်ပါသည်။

(၂) **ပရိုဂရမ်အသစ်တစ်ခု ရုတ်တရက်ပေါ်ပေါက်လာခြင်း။** အကယ်၍ အမျိုးအမည်မသိ ပရိုဂရမ်တစ်ခုသည် အသုံးပြုသူ၏ ကွန်ပျူတာပေါ်တွင် မကြာခဏပေါ်လာခဲ့လျှင် ဆိုက်ဘာတိုက်ခိုက်မှုခံနေရခြင်းဖြစ်ရန်များပါသည်။

(၃) **Utility ဆော့ဖ်ဝဲလ်များမှားယွင်းစွာအလုပ်လုပ်နေခြင်း။** အကယ်၍ Antivirus ပရိုဂရမ်တစ်ခု၊Task Manager နှင့် Registry Editor များကို ပိတ်ထားခံရပြီး ပြန်ဖွင့်၍မရခဲ့လျှင် ၎င်းကွန်ပျူတာသည်လည်း တိုက်ခိုက်ခြင်း ခံထားရပြီးဖြစ်ပါသည်။

(ဏ) **အသုံးပြုသူ၏ ကွန်ပျူတာသို့ ဝင်ရောက်နိုင်ရန် ဟက်ကာများ အသုံးပြုသည့် လွယ်ကူသော နည်းလမ်းများ**

(၁) **အခမဲ့ဆော့ဖ်ဝဲလ် Download ရယူခြင်းများ။** ဝယ်ယူရသည့် ဆော့ဖ်ဝဲလ် တစ်ခုခုကို အခမဲ့ရနိုင်ခြင်းသည် တရားမဝင်သည့်အပြင် မိမိကွန်ပျူတာ၏ လုံခြုံရေးကိုပါ အန္တရာယ်ဖြစ်စေနိုင်ပြီး အဖျက်အမှောင့်ပရိဂရမ်များဝင်ရောက်နိုင်ရန် တံခါးဖွင့်ပေးခြင်းလည်း ဖြစ်ပါသည်။ ထို့ကြောင့်လိုချင်သည့် ဆော့ဖ်ဝဲလ်အား ဝယ်ယူအသုံးပြုခြင်းက ပို၍လုံခြုံပါသည်။

(၂) **Cookie ခိုးယူမှုများ။** Cookie များက Login အချက်အလက်များ၊ အသုံးပြုထားသည့် ရာဇဝင်များအား မှတ်သားထားပါသည်။ ပုံမှန်ဖြစ်စေ၊ ဝှက်ထားခြင်းဖြစ်စေ Cookie များကို ရိုးရှင်းလှသော Browser Add-on တစ်ခုခုသုံးပြီးအလွယ်တကူခိုးယူခံရနိုင်ပါသည်။ဤပြဿနာအားဖြေရှင်းရန် အကောင်းဆုံးနည်းလမ်းမှာ ကောင်းမွန်စွာ တည်ဆောက်ထားသော၊ စိတ်ချရသော ဝက်ဘ်ဆိုက်များကိုသာ ကြည့်ရှုရန်ဖြစ်ပါသည်။

(၃) **အခမဲ့ပေးထားသော Wi-Fi များအား အသုံးပြုခြင်း။** ဘဏ်ကိစ္စများ၊ အွန်လိုင်းငွေလွှဲမှုများ၊ လူမှုကွန်ရက်များ အသုံးပြုရန် စသည်တို့အတွက် အခမဲ့ Wi-Fi များအသုံးပြုခြင်းသည် အန္တရာယ်များပါသည်။ ထို့ကြောင့် အများသုံး Wi-Fi ကွန်ယက်ထဲတွင် အသုံးပြုခဲ့လျှင် Virtual Private Network (VPN) ဆက်သွယ်မှုကိုသာအသုံးပြုရန် အကြံပြုပါသည်။

(တ) **တိုက်ခိုက်မှုအများစုကို ဟန့်တားနိုင်ရန် ဝန်ပေါ့သော နည်းလမ်းများ။** မတူညီသော ဝက်ဘ်ဆိုက်တိုင်းအတွက် ကွဲပြားသော Password များကို အသုံးပြုပါ။ မတူညီသော ဝက်ဘ်ဆိုက်တိုင်းတွင် ကွဲပြားသော Password များအား အသုံးပြုလေ့ရှိသောအကျင့်သည် အကောင့်တစ်ခု ပါသွားခဲ့လျှင်ပင် အချက်အလက် ခိုးယူခံရခြင်းမှအပြည့်အဝကာကွယ်ပေးနိုင်ပါသည်။အဓိကအသုံးပြုများသောPassword အားအခြားသောဝက်ဘ်ဆိုက်များတွင်အသုံးမပြုသင့်ပါ။Pop-upsများကိုလျစ်လျူ

ရှုထားပါ။ Pop-ups များကို ဝင်ခွင့်ပြုခြင်းက အဖျက်အမှောင့် ပရိုဂရမ်များကို Download လုပ်မိစေတတ်ပါသည်။ ထို့ကြောင့် E-commerce ကဲ့သို့သော ဝက်ဘ်ဆိုက်များပေါ်တွင် Site အားစစ်တမ်းကောက်ခြင်း ကဲ့သို့သော Pop-up များပြုလုပ်ခြင်းအား ရှောင်ရှားသင့်ပါသည်။ ဝက်ဘ်ဆိုက်များပေါ်တွင် အကောင့် အချက်အလက် အပြည့်အစုံသိမ်းထားခြင်းအား ရှောင်ကြဉ်ပါ။ ဝက်ဘ်ဆိုက်များသည် Password သိမ်းဆည်းရန်နှင့် လိုအပ်လျှင်အသုံးပြုနိုင်ရန် အခြားသော အချက်အလက်များကို တောင်းခံတတ်ပါသည်။ ထိုသို့သိမ်းဆည်းတတ်သော အလေ့ အကျင့်ရှိခြင်းက စီးပွားရေးဆိုင်ရာဆုံးရှုံးခြင်းများအထိ ဖြစ်စေနိုင်ပါသည်။

(ထ) **ဝက်ဘ်ဆိုက်များ အသုံးပြုရာတွင် စွန့်စားမှုများ လျှော့ချရန် နည်းလမ်းများ ပေါင်းစပ်ပါဝင်သည့် ဆော့ဖ်ဝဲလ်များအား Update လုပ်ပါ။** App၊ Widget၊ Plugin Version အဟောင်းများသည် ကောင်းမွန်စွာမလည်ပတ်နိုင်ကြဘဲ ဟက်ကာများအတွက် ဝင်ထွက်လွယ်သောလမ်းကြောင်းများ ဖြစ်နေတတ်ပါသည်။ ဝက်ဘ်ဆိုက်ရေးသူများသည် လက်ရှိထွက်ရှိနေသော ဆော့ဖ်ဝဲလ်Version များကိုသာ အသုံးပြုသင့်ပါသည်။ လုံခြုံစိတ်ချရသော Hosting ကုမ္ပဏီများကို ရွေးချယ်ပါ။ ဝက်ဘ်ဆိုက်တိုက်ခိုက်ခံရသည့် အန္တရာယ်နည်းပါးစေရန် ဝက်ဘ်ဆိုက်ပိုင်ရှင်များသည် ထူးခြားသောလုံခြုံမှုတိုင်းတာချက်များဖြင့် အလုပ်လုပ်ပြီး နောက်ဆုံးပေါ် Database နှင့် ပရိုဂရမ်များ အသုံးပြု၍ လုံခြုံရေးအလေးထားသော ကုမ္ပဏီများကိုသာရွေးချယ်သင့်ပါသည်။ Access ရယူခြင်းအားပိတ်ပင်ရန် ".htaccess"ကို အသုံးပြုပါ။ ".htaccess" ဖိုင်အား အသုံးပြု၍ ကိုယ်မသိသော IP Address များမှ Login စာမျက်နှာအား ဝင်ရောက်ခြင်းကို လွယ်ကူစွာပယ်ချနိုင်ပါသည်။ WordPress (သို့မဟုတ်) Content Management System (CMS) အခြေပြုဝက်ဘ်ဆိုက်များတွင် အသုံးပြုရန်အသင့်တော်ဆုံး၊ အကောင်းဆုံး နည်းလမ်းတစ်ခုလည်းဖြစ်ပါသည်။

(ဒ) **သမားရိုးကျ ဗိုင်းရပ်စ်တိုက်ဖျက်ရေးပရိုဂရမ်များသည် လုံလောက်သော ကာကွယ်မှု မပေးနိုင်ခြင်း ။** ဆိုက်ဘာတိုက်ခိုက်မှုအများစုသည် ကောင်းမွန်စွာစီမံပြုလုပ်

ထားပြီး သမားရိုးကျ ခြိမ်းခြောက်မှုများဖြင့်ယှဉ်၍ များစွာထူးခြားကွဲပြားနေကြ သောကြောင့် သမားရိုးကျ ဗိုင်းရပ်စ်တိုက်ဖျက်ရေး ပရိဂရမ်များမှ ကောင်းမွန်စွာ ကာကွယ်မှု မပေးနိုင်ကြပါ။ Online - Offline အန္တရာယ် ကိုင်တွယ်ဖြေရှင်းမှု ပရိဂရမ်များအား မရွေးချယ်လျှင် မည်သူမျှလုံခြုံရေးအား စိတ်ချမထားနိုင်ပါ။ စီးပွားဖြစ်ထုတ်လုပ်ထားသော ဖြေရှင်းနည်းလမ်းများကိုလူတိုင်းရနိုင်ပြီးဟက်ကာ များသည် ၎င်းလုံခြုံရေးစနစ်များကိုကြံဖန်နည်းလမ်းရှာဖွေ၍ လွယ်ကူစွာ ချိုးဖျက် နိုင်ပါသည်။ မျက်မှောက်ခေတ် ဟက်ကာများကမူ ပရိဂရမ်၏ အားနည်းချက်များ ထက်စာလျှင် Social Engineering ကိုအသုံးပြု၍ ဝါဒဖြန့်ချီရေး လက်နက်သဖွယ် အသုံးပြုတိုက်ခိုက်ကြပါသည်။ သမားရိုးကျဗိုင်းရပ်စ်တိုက်ဖျက်ရေးပရိဂရမ်များသည် ထိုကဲ့သို့ တိုက်ခိုက်မှုမျိုးအား ကာကွယ်နိုင်ခဲ့ပါသည်။

(ခ) **ဆိုက်ဘာတိုက်ခိုက်မှုများအားရှောင်ရှားနိုင်ရန်နှင့်နိုးကြားမှုရှိစေရန်နည်းလမ်းများ**

(၁) **လူမှုကွန်ယက်ပေါ်တွင်တင်ထားသော မေးခွန်းလင့်ခ်များ၊ ဖောင်များကို စေ့စပ်စွာစစ်ဆေးပါ။** အကယ်၍ တစ်စုံတစ်ယောက်က သံသယဖြစ်ဖွယ်ရာ လင့်ခ်တစ်ခုကိုတင်ထားလျှင်၎င်းလင့်ခ်ကို မနှိပ်ခြင်းက ပိုကောင်းပါသည်။ ဟက်ကာများသည် အဖျက်အမှောင့်ဆော့ဖ်ဝဲလ်အား အတိုင်းအတာတစ်ခုထိ ပုံနှံ့စေရန် ထိုကဲ့သို့ လင့်ခ်များကိုအသုံးပြုပါသည်။

(၂) **ကြွေးဝယ်စာရင်းထုတ်ပြန်ချက်များကို သေချာစွာစောင့်ကြည့်ပါ။** အကြွေး စာရင်းထုတ်ပြန်ချက်များကို ပုံမှန်စောင့်ကြည့်ခြင်းအားဖြင့် ပုံမှန်မဟုတ်သော အခြေအနေများကို လွယ်လင့်တကူ သိမြင်နိုင်စေသောကြောင့် သက်သေခံ အချက်အလက်များ ခိုးယူခံရခြင်းမှ ကာကွယ်နိုင်ပါသည်။ ဝယ်သူများနှင့် သက်ဆိုင်သော အချက်အလက်များကိုသာ ထိန်းသိမ်းထားသင့်ပါသည်။ ဝယ်သူများနှင့် သက်ဆိုင်သော အချက်အလက်များကိုသာ ရယူထားခြင်းသည် အဆိုးဝါးဆုံး အခြေအနေဖြစ်လျှင်ပင် ဆုံးရှုံးခြင်းပမာဏများနှင့် သက်သေခံ အချက်အလက်များခိုးယူခံရခြင်းများကို လျော့နည်းသက်သာစေပါသည်။

(၃) **နည်းပညာမြှင့်ပစ္စည်းများအား သတိထား၍ အသုံးပြုပါ။** စမတ် နာရီများကဲ့သို့ နည်းပညာမြင့် အသုံးအဆောင်ပစ္စည်းများသည် ကွန်ပျူတာ အရံပစ္စည်းများနှင့် ချိတ်ဆက်မှုများပြုလုပ်၍ ပင်မ Application များကို အသုံးပြုသောကြောင့် ဟက်ကာတစ်ယောက်သည် ထိုပင်မ Application များကိုသိမ်းပိုက်နိုင်ရုံဖြင့် ၎င်းတို့နှင့်ချိတ်ဆက်ထားသော စက်ပစ္စည်းများ၊ အချက်အလက်များအားလုံးကို ရယူနိုင်ပါသည်။ ထို့ကြောင့် တရားမဝင် ဆော့ဖ်ဝဲလ်များဖြင့်ထုတ်လုပ်ထားသော စက်ပစ္စည်းများကို အသုံးမပြုရန် အရေးကြီးပါသည်။

(၄) **အဖျက်အမှောင့် ဆော့ဖ်ဝဲလ်။** ဆိုက်ဘာ ရာဇဝတ်မှုကျူးလွန်သူများ၏ ထူးခြားသတ်မှတ်ထားသော အဖျက်အမှောင့်ပရိဂရမ်ဆိုသည်မှာ Scareware၊ Spyware၊ Ransomware၊ Worms၊ ကွန်ပျူတာဗိုင်းရပ်စ်စသည့် အလိုအလျောက်ရောက်ရှိလာတတ်သောဆော့ဖ်ဝဲလ်များကိုခြုံ၍ခေါ်ဝေါ်ခြင်းဖြစ်ပါသည်။ Adware ကဲ့သို့ ဆော့ဖ်ဝဲလ်များသည်လည်း ၎င်းအဖျက်အမှောင့်ဆော့ဖ်ဝဲလ်အုပ်စုထဲတွင် ပါဝင်ပါသည်။ Social Engineering လုပ်ခြင်းဖြင့်ဖြစ်စေ၊ ကွန်ပျူတာ၏အားနည်းချက်များကိုရှာ၍ ထိုးဖောက်ခြင်းများဖြင့်ဖြစ်စေ ဆိုက်ဘာတိုက်ခိုက်မှုများ ပြုလုပ်ရာတွင် ဆန်းသစ်သော အဖျက်အမှောင့် ဆော့ဖ်ဝဲလ်များကို အသုံးပြုကြပါသည်။ Gozi၊ Vawtrack၊ Dridex များမှာ ဘဏ်များအား တိုက်ခိုက်ရာတွင် အသုံးပြုခဲ့သည့် အဆင့်မြင့်အဖျက်အမှောင့် ဆော့ဖ်ဝဲလ်များဖြစ်ပါသည်။ဖိုင်များ ပြောင်းလဲနေခြင်း၊ ပျောက်ဆုံးနေခြင်း၊ CPU အသုံးပြုမှုများ မြင့်မားလာခြင်း၊ မကြာခဏ ကွန်ပျူတာ ထိုးရပ်သွားခြင်း စသည်တို့သည် အဖျက်အမှောင့် ဆော့ဖ်ဝဲလ်များ တိုက်ခိုက်ခံရမှု၏ အခြေခံလက္ခဏာများဖြစ်ပါသည်။[9]

[9] Available from: https://www.mmcert.org.mm/node/340 [accessed 3 May 2018]

မြန်မာနိုင်ငံအပေါ် ဆိုက်ဘာတိုက်ခိုက်မှုများ

၂၄။ မြန်မာနိုင်ငံအနေဖြင့် ၂၀၁၀ ပြည့်နှစ်နှင့် ၂၀၁၇ခုနှစ်များတွင် (နှစ်ကြိမ်) ဆိုက်ဘာတိုက်ခိုက်မှုနှင့်ရင်ဆိုင်ခဲ့ရပါသည်။ ၂၀၁၀ ပြည့်နှစ် အောက်တိုဘာလအတွင်း တိုက်ခိုက်မှုသည် မြန်မာနိုင်ငံရွေးကောက်ပွဲမတိုင်မီ အင်တာနက်အဆက်အသွယ်များကို နှောင့်ယှက်ရန်အတွက် တိုက်ခိုက်မှုများပြုလုပ်ခဲ့ခြင်းဖြစ်သည်။ ၎င်းတိုက်ခိုက်မှုသည် ၂၀၀၇ ခုနှစ်တွင်အက်စတိုးနီးယားနိုင်ငံနှင့် ၂၀၀၈ ခုနှစ်တွင် ဂျော်ဂျီယာနိုင်ငံတို့တွင် ဖြစ်ပွားခဲ့သောတိုက်ခိုက်မှုများထက် ပိုမိုကြီးမားပါသည်။ မြန်မာနိုင်ငံ၏အဓိက အင်တာနက်ထောက်ပံ့သူဖြစ်သည့် MPT (Ministry of Post and Telecommunication) နှင့် ရတနာပုံတယ်လီပို့ကုမ္ပဏီကို အဓိကထားတိုက်ခိုက်ခဲ့ခြင်းဖြစ်သည်။ အဆိုပါတိုက်ခိုက်မှုသည် အဓိကကျသည့် အဝင်၊ အထွက် ကွန်ရက်အသွားအလာတို့ကို နှောင့်ယှက်ခဲ့သည်။ ထို့ပြင် ရေကြောင်းမှ ဆက်သွယ်ထားသည့် ကေဘယ်ကြိုးသည် မတော်တဆဖြစ်ခဲ့ရာမှ အင်တာနက်အဆက်အသွယ်များ ပြတ်တောက်သွားခဲ့ရသည့် ဖြစ်ရပ်များလည်း ပေါ်ပေါက်ခဲ့သည်။ ၂၀၁၇ ခုနှစ်ဖြစ်စဉ်သည် ရခိုင်ဒေသတွင် ဖြစ်ပွားနေသော အခြေအနေများနှင့်ပတ်သတ်၍ မြန်မာနိုင်ငံအပေါ်ပစ်မှတ်ထားပြီး ဆိုက်ဘာတိုက်ခိုက်မှု ပြုလုပ်ခဲ့ခြင်းဖြစ်သည်။ တူရကီနှင့်အင်ဒိုနီးရှားအခြေစိုက် ဟက်ကာများက နိုင်ငံတော်သမ္မတရုံး ဝက်ဘ်ဆိုက် အပါအဝင် မြန်မာဝက်ဘ်ဆိုက် ၂၂ ခုကို ၂၀၁၇ ခုနှစ် စက်တင်ဘာလတွင် တိုက်ခိုက်ခဲ့ပြီး မြန်မာဟတ်ကာများကလည်း တူရကီဝက်ဘ်ဆိုက် ၇၀၀ကျော်ကို ပြန်လည်တိုက်ခိုက်ခဲ့ပါသည်။[10]

၂၀၁၇ ခုနှစ် နှင့် ၂၀၁၈ ခုနှစ်တွင် နိုင်ငံအချို့၏ ဆိုက်ဘာလုံခြုံရေးနှင့် ပတ်သတ်သော ကိန်းဂဏန်း အချက်အလက်များ

၂၅။ ကမ္ဘာပေါ်တွင် ဆိုက်ဘာတိုက်ခိုက်မှု ဖြစ်စဉ်များ တစ်နေ့တစ်ခြားများပြားလာလျက်ရှိပါသည်။ အရေးကြီးရွေးကောက်ပွဲမှအစ လုပ်ငန်းတော်တော်များများတွင် ပါဝင်ပတ်သက်မှုရှိနေပြီး နေ့စဉ်လူမှုဘဝကို ခြိမ်းခြောက်နေမှုများကို လျှော့တွက်၍မရပါ။

၂၆။ ဖော်ပြပါစာရင်းအချက်အလက်များသည် ၂၀၁၈ ခုနှစ်တွင် ထုတ်ပြန်သော Microsoft နှင့် သုတေသနစာတမ်းများအရ ဖော်ပြထားခြင်းဖြစ်ပါသည် -

[10] Available from: http://thevoicemyanmar.com/it/11597-trk [accessed 8 May 2018]

(က) ၂၀၁၆ ခုနှစ်တွင် အမေရိကန်အစိုးရသည် Cyber Security အတွက် အမေရိကန် ဒေါ်လာ ၂၈ ဘီလီယံအထိသုံးစွဲခဲ့ပြီး ၂၀၁၇၊ ၂၀၁၈ ခုနှစ်တို့တွင်ပို၍ သုံးစွဲလာနိုင်သည်ဟု ခန့်မှန်းကြသည်။

(ခ) Microsoft ၏ အချက်အလက်များအရ ကမ္ဘာ့အဖွဲ့အစည်းအသီးသီး၏ ဆိုက်ဘာမှုခင်းများအတွက် ကုန်ကျစရိတ်မှာ အမေရိကန် ဒေါ်လာ ၅၀၀ ဘီလီယံပမာဏထက် ကြောက်မက်ဖွယ်ရာရှိနေပြီး ကုမ္ပဏီတစ်ခုချင်း ပျမ်းမျှ Data ဖောက်ထွင်းခံရမှုကြောင့် ပျမ်းမျှကုန်ကျငွေသည် အမေရိကန် ဒေါ်လာ ၃.၈ ဘီလီယံရှိပါသည်။

(ဂ) Data ဖောက်ထွင်းခံရမှုများကြောင့် ပျမ်းမျှကုန်ကျစရိတ်များသည် ၂၀၁၅ ခုနှစ်မှ ၂၀၂၀ ခုနှစ်တွင် လေးဆခန့် ပိုမိုမြင့်တက်သွားနိုင်ဖွယ်ရာရှိပါသည်။

(ဃ) ၂၀၁၇ ခုနှစ်တွင် Ranson warp တိုက်ခိုက်ခံရမှုသည် ၃၆ ရာခိုင်နှုန်း တိုးလာခဲ့ပါသည်။

(င) Ranson warp တိုက်ခိုက်ခံရပြီးနောက် ပျမ်းမျှ ပြန်ပေးငွေပမာဏသည် အမေရိကန် ဒေါ်လာ ၁၀၇၇ ဖြစ်ပါသည်။

(စ) ဟတ်ကာများသည် e-mail အသုံးများလာပြီး e-mail ၁၃၁ ခုတွင် Malware Virus ၁ ခု ပါဝင်ပါသည်။

(ဆ) ၂၀၁၇ ခုနှစ်စစ်တမ်းများအရ လိမ်လည်လှည့်စားဖျားယောင်းခံရသူမှာ ၆.၅ ရာခိုင်နှုန်းရှိပြီး ယခင်နှစ်ထက်စာလျှင် နှစ်ဆခန့် များပြားလာခြင်းဖြစ်သည်။

(ဇ) ဆိုက်ဘာတိုက်ခိုက်မှု ၄၃ ရာခိုင်နှုန်းသည် လုပ်ငန်းငယ်များကို ဦးတည်ပါသည်။

(ဈ) ဆိုက်ဘာဖြစ်စဉ်များကြောင့် ဆိုက်ဘာလုံခြုံရေးကို အလေးထား ဆက်နွယ်လာသောလုပ်ငန်းအရေအတွက်များ တိုးမြှင့်လာရာ ၂၀၂၁ ခုနှစ်တွင် ၃.၅ ရာခိုင်နှုန်းထိ ရှိလာနိုင်ပါသည်။

(ည) သန်းကြွယ်သူဌေး **WARREN BUFFETT** ၏ အဆိုအရ လူသားတို့အပေါ် ဆိုက်ဘာအန္တရာယ်ကျရောက်ခြင်းသည် နျူးကလီးယားအန္တရာယ်ထက် ပိုမိုကြီးမားသည်ဟု ဆိုပါသည်။

(၎) Malware ဗိုင်းရပ်စ်အသစ်နမူနာ ၂၃၀၀၀၀ ကို နေ့စဉ်ထုတ်လုပ်နေမှုသည် ဗိုင်းရပ်စ် အသစ်များ ကြီးထွားလာမှုကို ဖော်ပြနေပါသည်။

(၅) တရုတ်နိုင်ငံသည် ကမ္ဘာပေါ်တွင် Malware ဗိုင်းရပ်စ် အန္တရာယ်ပေးမှုအများဆုံး နိုင်ငံဖြစ်ပါသည်။

(၃) ပြန်ပေးငွေတောင်းခံတိုက်ခိုက်မှု ဖြစ်စဉ်များသည် နေ့စဉ် ၄၀၀၀ ကျော်ထိရှိသည် ကိုတွေ့ရှိရပါသည်။

(၀) ၇၈ ရာခိုင်နှုန်းရှိသောသူများတွင် မိမိတို့မသိသော e-mail link ကိုလက်ခံခြင်းဖြင့် များစွာသော Link များကို လက်ခံမိခြင်းကဲ့သို့သော အန္တရာယ်များရှိကြောင်းကို သိရှိရပါသည်။

(၈) ၉၀ ရာခိုင်နှုန်းသော Hacker များသည် ၎င်းတို့၏ထောင်ချောက်များကို အများ နားမလည်အောင် ဖတ်၍မရသော အက္ခရာများအသုံးပြုခြင်းဖြင့် ဖုံးကွယ်ထားပါသည်။

(တ) မိမိ၏ Data များချိုးဖောက်ခံရလျှင် စုံစမ်းစစ်ဆေးမှုကို ၁၉၇ ရက်ခန့် အချိန်ယူ၍ စစ်ဆေးရကြောင်းသိရှိရပါသည်။

(ထ) Android System သည် Windows စနစ်များနောက်တွင် ဒုတိယနောက်ယှက်ခံ ရသော ပစ်မှတ်ဖြစ်သည်။

(ဒ) သတင်းအချက်အလက်ဖောက်ထွင်းခံရသော ပစ်မှတ် ၈၁ ရာခိုင်နှုန်းသည် မိမိ ကိုယ်တိုင်ဖောက်ထွင်းခံရမှုကို စုံစမ်းဖော်ထုတ်သည့် စနစ်များမရှိကြပါ။

(ဓ) ၉၅ ရာခိုင်နှုန်းသော အမေရိကန်လူမျိုးများသည် ကုမ္ပဏီများတွင် ၎င်းတို့၏ အချက် အလက်များ မည်သို့မည်ပုံအသုံးပြုရမည် ဆိုသည်နှင့်ပတ်သက်၍ ပါဝင်ပတ်သက် နေကြသည်။

(န) Virtual Private Networks (VPNs) အား ပြည်သူများက အများဆုံးအသုံးပြု ရသည့်အကြောင်းမှာ အမည်မဖော်ပြသူများ၏ ခေါင်းစဉ်များကို အကြမ်းဖျင်းကြည့်ရှု နိုင်ခြင်းနှင့်ဖျော်ဖြေရေးကဏ္ဍများကိုထိန်းချုပ်ထားခြင်းမရှိခြင်းတို့ကြောင့်ဖြစ်ပါသည်။

(ပ) (VPNs) သုံးစွဲသူ ၄၂ ရာခိုင်နှုန်းသည် VPN တစ်ခုကို တစ်ပတ်လျှင်အနည်းဆုံး ၄ ကြိမ်မှ ၅ ကြိမ်ထိသုံးစွဲကြသည်။[11]

နိဂုံး

၂၇။ ဖွံ့ဖြိုးဆဲနိုင်ငံဖြစ်သော မြန်မာနိုင်ငံအနေဖြင့် အိမ်နီးနားချင်းနိုင်ငံများတွင် သာမက အာဆီယံနိုင်ငံများနှင့်ပါ ရင်ဘောင်တန်းနိုင်ရန်အတွက် နိုင်ငံတော်မှ ရည်မှန်းချက်များ၊ မူဝါဒများချမှတ်ဆောင်ရွက်လျှက်ရှိပါသည်။ နိုင်ငံတော်၏ အုပ်ချုပ်ရေး၊ လူမှုရေး၊ စီးပွားရေး ကဏ္ဍအသီးသီး ဟန်ချက်ညီစွာ ဖွံ့ဖြိုးတိုးတက်စေရန်အတွက် e-Government လုပ်ငန်းစဉ်များကို ၂၀၀၀ ခုနှစ်မှစတင်၍ ချမှတ်ဆောင်ရွက်လျှက်ရှိပါသည်။ထင်းလုပ်ငန်းစဉ်များ ဖွံ့ဖြိုးတိုးတက်လာမှုနှင့်အတူ ဆိုက်ဘာလုံခြုံရေးနှင့် ပါတ်သတ်သည့်လုပ်ငန်းများဖြင့်လည်း ပိုမိုထိရောက်စွာ ကာကွယ်နိုင်ရမည် ဖြစ်ပါသည်။ မြန်မာနိုင်ငံရှိ ဝန်ကြီးဌာနများအနေဖြင့်လည်း ၎င်းတို့၏ ဆောင်ရွက်ချက်များကို ပွင့်လင်းမြင်သာစွာဖြင့် ပြည်သူလူထုသိရှိစေရန် ဝက်ဘ်ဆိုက်များ၊ လူမှုကွန်ရက်စာမျက်နှာများတွင် အချိန်နှင့်တပြေးညီ နိုင်ငံအတွင်းသာမက လိုအပ်လျှင် ကမ္ဘာနိုင်ငံများသို့ပါ သတင်းထုတ်ပြန်ရန်လိုအပ်ပါသည်။ လက်ရှိကြုံတွေ့နေရသော ရခိုင်ပြည်နယ် ဖြစ်စဉ်သည် အချိန်နှင့်တပြေးညီ သတင်းထုတ်ပြန်ရန်အားနည်းခြင်း၊ သတင်းအတည်ပြုစီစစ်ရာတွင် နှောင့်နှေးခြင်း၊ထုတ်ပြန်၍မရအောင် သမ္မတရုံးဝက်ဘ်ဆိုက်အပါအဝင် ဝန်ကြီးဌာနဝက်ဘ်ဆိုက်များ ဆိုက်ဘာတိုက်ခိုက်ခံရခြင်းတို့ကြောင့် အစိုးရမှသတင်းထုတ်ပြန်ချိန်သည် မမှန်သတင်းများ ဖတ်ရှုပြီးချိန်ဖြစ်နေခြင်းကြောင့် သတင်းမှားများအား နိုင်ငံတကာမှလက်ခံပြီး ဖိအားပေးခြင်းခံရပါသည်။ ပို့ဆောင်ရေးနှင့်ဆက်သွယ်ရေးဝန်ကြီးဌာနမှ အကောင်အထည်ဖော် ဆောင်ရွက်မည့် Myanmar e-Government Master Plan လုပ်ငန်းများ ဖွံ့ဖြိုးတိုးတက်လာသည်နှင့်အမျှ ပြည်သူပိုင်နှင့် နိုင်ငံပိုင်ဖြစ်သော နည်းပညာလုပ်ငန်းနှင့် ဆက်နွယ်နေသော ထုတ်လုပ်မှုနှင့် ရောင်းလိုအားလည်းမြှင့်တင်လာမည်ဖြစ်ပါသည်။ ၎င်းမှတဆင့် ဥပဒေများ၊ နည်းဥပဒေများ၊ ရေးဆွဲထုတ်ပြန်ပြီး နည်းပညာကို အခြေခံသောလုပ်ငန်းများဖြင့် နိုင်ငံတော်၏လုံခြုံရေးနှင့် စီးပွားရေးဖွံ့ဖြိုးတိုးတက်

[11] Available from: https://thebestvpn.com/cyber-security-statistics-2018/ [accessed 15 May 2018]

မှုတွင် အဓိကအရေးကြီးသော အခန်းကဏ္ဍသို့ရောက်ရှိပြီးနောက် ဆိုက်ဘာလုံခြုံရေးကဏ္ဍကိုလည်း ပိုမိုအောင်မြင်အောင် ဆောင်ရွက်လာနိုင်မည်ဖြစ်ကြောင်းတင်ပြအပ်ပါသည်။

ဤစာတမ်းတိုအား ဦးဝင်းဇော်လတ်(ဒုတိယညွှန်ကြားရေးမှူး)မှ တာဝန်ယူရေးသားပြီး သုတေသနဌာနရှိ အရာထမ်းအဆင့်ဆင့်မှ ဝိုင်းဝန်းကြိုးကြပ်တည်းဖြတ်၍ ထုတ်ဝေခြင်းဖြစ်ပါသည်။

သုတေသနဌာန

ပြည်သူ့လွှတ်တော်ရုံး

သတိပြုရန်

ဤသတင်းအချက်အလက်သည် လွတ်တော်ကိုယ်စားလှယ်များအား ၎င်းတို့၏ လွတ်တော်ဆိုင်ရာ တာဝန်များကို ဆောင်ရွက်ရာတွင် အထောက်အကူပြုရန်အတွက် ဖြစ်ပါသည်။ ပုဂ္ဂိုလ်ရေးဆိုင်ရာ ကိစ္စ တစ်စုံတစ်ခုအတွက် အသုံးပြုရန်မဟုတ်ပါ။ အချိန်နှင့်တပြေးညီ နောက်ဆုံးရသတင်းဖြစ်မည်ဟု သတ်မှတ် မထားသင့်ပါ။ ဤအချက်အလက်များအား တရားဝင် သို့မဟုတ် ပညာရှင်ဆိုင်ရာအကြံပေးချက်အဖြစ် မသတ်မှတ်သင့်ပါ။ အထူးအကြံပေးချက် သို့မဟုတ် သတင်းအချက်အလက်များလိုအပ်ပါက အရည် အသွေးပြည့်မီသော သင့်လျော်သည့် ကျွမ်းကျင်ပညာရှင်နှင့် ဆွေးနွေးတိုင်ပင်သင့်ပါသည်။ လွတ်တော် သုတေသနဝန်ဆောင်မှုသည် စာတမ်းတိုများတွင် ပါဝင်သောအကြောင်းအရာများနှင့်စပ်လျဉ်း၍ လွတ်တော် ကိုယ်စားလှယ်များ၊ လွတ်တော်ဝန်ထမ်းများနှင့် ဆွေးနွေးမှုများ ပြုလုပ်ပေးနိုင်ပါသည်။ အများပြည်သူနှင့် ဆွေးနွေးမှုများ ပြုလုပ်ခြင်းမရှိပါ။