Password ပေးရာတွင် သိသင့်သည့်အခြေခံအချက်များ

- မိမိတို့၏ သတင်းအချက်အလက်များ လုံခြုံစေရန်အတွက် သူတစ်ပါးအလွယ်တကူ မခန့်မှန်းနိုင်သောPassword များကို အသေအချာပေးသင့်ပါသည်။

- Password များ ပေးရာတွင် မိမိတို့ကိုယ်ရေးကိုယ်တာများနှင့် သက်ဆိုင်သော အမည်များ၊ တယ်လီဖုန်းနံပါတ်များ၊ မွေးနေ့ရက်စွဲများ၊ Credit ကဒ်နံပါတ်များ၊ လိပ်စာများ စသည်ဖြင့် မပေးသင့်ပါ။

- သင်္ကေတများ၊ ဂဏန်းများ၊ အက္ခရာ အကြီးအသေးများ ပေါင်းစပ်၍ မိမိတို့၏ Password များကို ပေးသင့်ပါသည်။

အင်တာနက်အသုံးပြုသူများ သတိပြုလိုက်နာရမည့်အချက်များ

- ပုဂ္ဂိုလ်ရေးအချက်အလက်များနှင့် ငွေကြေးဆိုင်ရာ အချက်အလက်များကို တောင်းခံသည့် Link များတွင်ယုံကြည်စိတ်ချရသော Website ဟုတ်၊မဟုတ် စစ်ဆေးပြီးမှသာ ဖြည့်စွက်ရမည်။

- မိမိ၏အဖွဲ့အစည်းတွင်းရှိသော သတင်းအချက်အလက်များ၊ ပုဂ္ဂိုလ်ရေးဆိုင်ရာ သတင်းအချက်အလက်များနှင့် ကွန်ရက်တည်ဆောက်ပုံများကို တာဝန်ရှိသူ၏ ခွင့်ပြုမိန့်မပါဘဲ ယူဆောင်ခြင်း၊ လွှဲပြောင်းခြင်းများ မပြုလုပ်ရ။

- အရေးကြီးသောအချက်အလက်များကို အင်တာနက်မှတစ်ဆင့် ပေးပို့ရာတွင် Password ခံ၍ ပေးပို့ရမည်ဖြစ်ပြီး Password ကိုSMS မှတစ်ဆင့် ပေးပို့ရမည်။

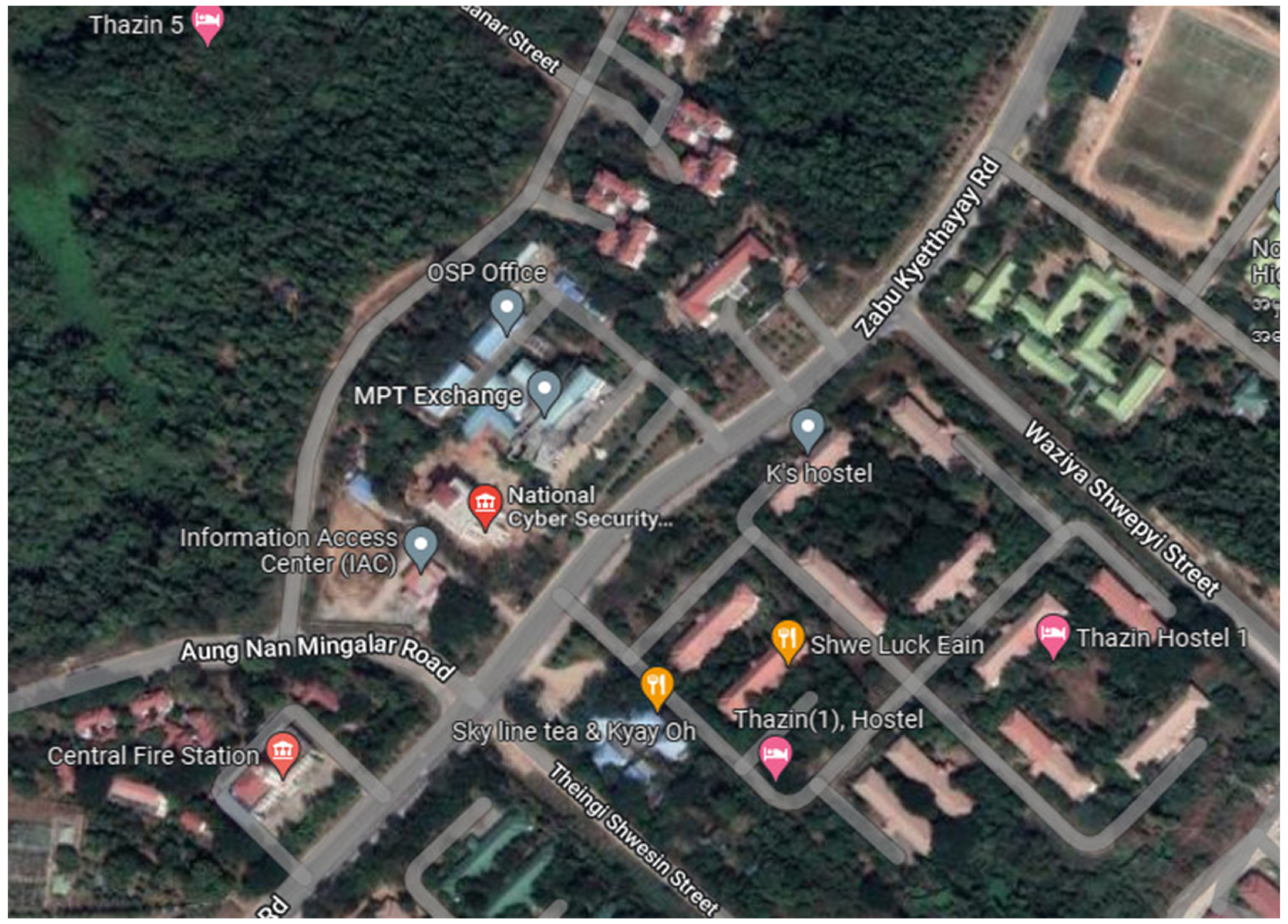
ဆက်သွယ်ရန်လိပ်စာ

ဖုန်း - ၀၆၇-၃၄၂၂၂၇၂

နေရာ - NCSC Building, ဇမ္ဗူကျက်သရေလမ်း၊
ဇမ္ဗူသီရိမြို့နယ်၊ နေပြည်တော်။

Email - infoteam@mmcert.org.mm

Website - https://www.mmcert.org.mm



mmCERT
MYANMAR COMPUTER EMERGENCY RESPONSE TEAM

Ministry of Transport and Communications
ပို့ဆောင်ရေးနှင့်ဆက်သွယ်ရေးဝန်ကြီးဌာန

mmCERT ဆိုသည်မှာ

- သတင်းအချက်အလက်နှင့် အင်တာနက်လုံခြုံရေးဆိုင်ရာ ပြဿနာများတွင်အရေးပေါ်တုံ့ပြန်မှုပြုလုပ်ရန် ရည်ရွယ်၍ဖွဲ့စည်းထားသည့် အဖွဲ့အစည်းတစ်ခု ဖြစ်ပါသည်။

- နိုင်ငံတော်အဆင့် အဖွဲ့အစည်းတစ်ခုဖြစ်ပြီး နိုင်ငံတကာ CERT အဖွဲ့အစည်းများနှင့်ဆက်သွယ်၍ သတင်းအချက်အလက်၊ အင်တာနက်လုံခြုံရေးကို တရားဝင်ဆောင်ရွက်လျက်ရှိပါသည်။ ထို့ပြင် အင်တာနက်သုံးစွဲသူများအား ဆိုက်ဘာလုံခြုံရေးအသိပညာဗဟုသုတများနှင့် နည်းပညာအထောက်အပံ့များ ပေးနိုင်ရန်ရည်ရွယ်ပါသည်။

- mmCERT ကို ၂၀၀၄ ခုနှစ်၊ ဇူလိုင်လ ၂၃ ရက်နေ့တွင် ဖွဲ့စည်းခဲ့ပါသည်။

mmCERT တာဝန်

- ဆိုက်ဘာလုံခြုံရေးနှင့်ဆိုက်ဘာရာဇဝတ်မှုများအတွက် နိုင်ငံတကာCERT များနှင့် ပူးပေါင်းဆောင်ရွက်၍ နိုင်ငံ၏ IT Image ကို ဖော်ဆောင်ရန်။

- ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ သတင်းအချက်အလက်များနှင့် အကြံဉာဏ်များဖြန့်ဝေပေးရန်။

- နည်းပညာအကူအညီများပေးရန်။

- ဆိုက်ဘာရာဇဝတ်မှုများအတွက်ဥပဒေပိုင်းဆိုင်ရာအဖွဲ့အစည်းများနှင့်ပူးပေါင်းဆောင်ရွက်ရန်။

mmCERT မြန်မာနိုင်ငံကွန်ပျူတာအရေးပေါ်တုံ့ပြန်ရေးအဖွဲ့

Ransomware နှင့်ပတ်သက်၍ သိကောင်းစရာများ

➤Ransomware ဆိုသည်မှာ ကွန်ပျူတာတွင်းရှိဖိုင်များကို ဖွင့်မရအောင်ပြုလုပ်ပြီး ဖိုင်များကို ပြန်လည်ရရှိလိုပါက ငွေပေးချေမှုပြုလုပ်ရသော ပရိုဂရမ်တစ်မျိုးဖြစ်ပါသည်။ တောင်းခံသော ငွေအမျိုးအစားမှာ များသောအားဖြင့် Crypto ငွေကြေးဖြစ်သော BitCoin ဖြစ်ပြီး ပေးချေရသော ငွေပမာဏမှာ ဒေါ်လာ ၃၀၀ မှ ဒေါ်လာ သန်း ၅၀ အထိ ဖြစ်နိုင်ပါသည်။

➤မြန်မာနိုင်ငံတွင် STOP Ransomware တိုက်ခိုက်ခံရမှုသည် အများဆုံး ဖြစ်ပြီး ဖိုင်များကို ပြန်လည်ရရှိရန်အတွက် ပေးချေရသောငွေပမာဏမှာ ဒေါ်လာ ၄၉၀ မှ ဒေါ်လာ ၉၈၀ နှင့်ညီမျှသော BitCoin ဖြစ်ပါသည်။

➤တရားမဝင်ဆော့ဖ်ဝဲလ်များကို အင်တာနက်တွင် Download လုပ်မိရာမှ၊ Crack ဖိုင်များကို Download လုပ်မိရာမှ ထိုပရိုဂရမ်များမှတစ်ဆင့် STOP Ransomware တိုက်ခိုက်ခံရခြင်း ဖြစ်ပါသည်။ ပြည်တွင်းတွင် လိုင်စင်ပါရှိသော ဆော့ဖ်ဝဲလ်များကိုအသုံးပြုသူနည်းပါးခြင်းသည် Ransomware တိုက်ခိုက်ခံရခြင်း၏ အဓိက အကြောင်းရင်း ဖြစ်ပါသည်။

➤Ransomware တိုက်ခိုက်ခံရမှုမှကာကွယ်ရန် အောက်ပါအချက်များကို လိုက်နာရမည်–

(က) Microsoft Windows တွင်ပါရှိသော Windows Defender တစ်ခုတည်းအား အသုံးပြုခြင်းအစား အခြားသော Antivirus များ(ESET၊ Kaspersky၊ BitDefender စသည်)ကို အသုံးပြုရန် လိုအပ်ပြီး Virus Definition များကို နောက်ဆုံးအခြေအနေအထိ update ပြုလုပ်ထားရန် လိုအပ်ပါသည်။

(ခ) မည်သည့်အကြောင်းရင်းဖြင့်မျှ Antivirus ကို မပိတ်ရ။

(ဂ) မယုံကြည်ရသောWebsite များမှ မလိုအပ်ဘဲ ဖိုင်များကိုDownload လုပ်ခြင်း မပြုရ။

(ဃ) System Restore point ကို Volume Drive အားလုံးတွင် ထားရှိသင့်ပါသည်။

(င) အရေးကြီးသော ဖိုင်များကို encryption အသုံးပြု၍ အခြားသော External Storage များတွင် သိမ်းဆည်းခြင်း၊ Cloud တွင် သိမ်းဆည်းခြင်းမျိုး ပြုလုပ်ပါ။

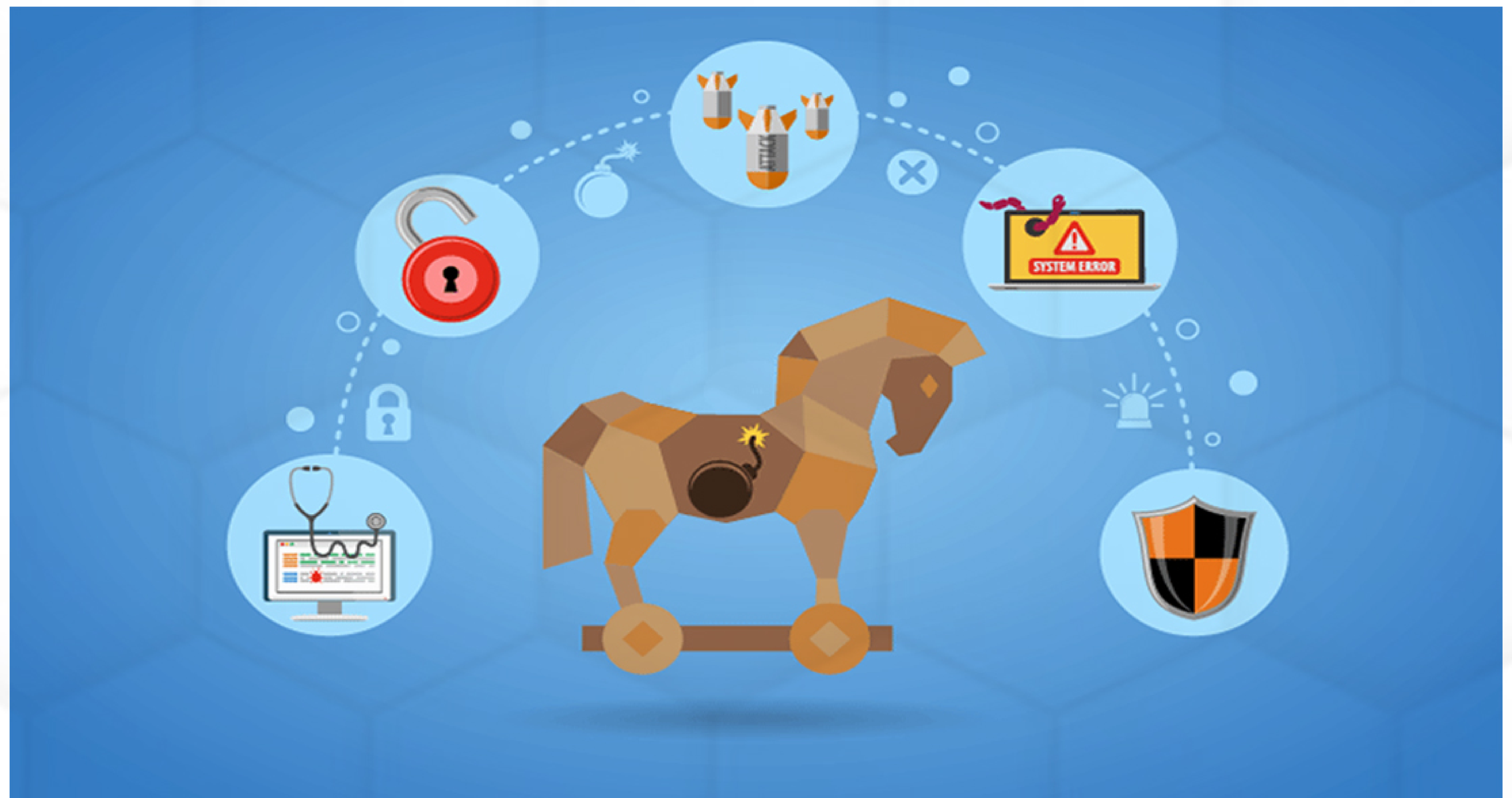
(စ) အဖွဲ့အစည်းအတွင်း Ransomware နှင့်ပတ်သက်၍ အသိပညာပေးဆွေးနွေးမှုမျိုးလုပ်ဆောင်ပါ။

Remote Access Trojan အကြောင်း သိကောင်းစရာများ

➤Remote Access Trojan (RAT) ဆိုသည်မှာ ကွန်ပျူတာတွင်း တိတ်တဆိတ်ဝင်ရောက်ကာ အဆိုပါကွန်ပျူတာအား အဝေးမှနေ၍ ထိန်းချုပ်နိုင်သော ပရိုဂရမ် ဖြစ်ပါသည်။

➤Mustang Panda ဟက်ကာအဖွဲ့သည် ၂၀၁၄ ခုနှစ်မှစ၍ အာရှ–ပစိဖိတ်ဒေသတွင်း နိုင်ငံများအား ပစ်မှတ်ထား၍ ဆိုက်ဘာတိုက်ခိုက်ပြီး သတင်းအချက်အလက်များကို ခိုးယူရန် ကြိုးစားလျက်ရှိကာ ၂၀၁၉ ခုနှစ်တွင် မြန်မာနိုင်ငံကို ပစ်မှတ်ထား၍ PlugX RAT ဖြင့် တိုက်ခိုက်ခဲ့ပြီး မြန်မာနိုင်ငံအတွင်းရှိ ကွန်ပျူတာအများစုသည် PlugX RAT ၏တိုက်ခိုက်ခြင်း ခံရလျက်ရှိပါသည်။

➤PlugX RAT မျိုးကွဲများသည် မူလအစတွင် Phishing Mail များမှတဆင့် စိတ်ဝင်စားဖွယ်ရာ Attachment ဖိုင်များအနေဖြင့် ရောက်ရှိလာခြင်းဖြစ်ပြီး Email လက်ခံရရှိသူသည် အဆိုပါ Attachment ဖိုင်ကိုဖွင့်မိရာမှ Attachment တွင်ပါလာသော အဖျက်အမှောင့်ကုဒ်များမှ စတင်အလုပ်လုပ်ပြီး ကွန်ပျူတာတွင် ခြေကုပ်ယူပါသည်။ ထို့နောက် ကွန်ပျူတာသို့ လာရောက်ချိတ်ဆက်သော Memory Stick နှင့် External Hard Disk ကဲ့သို့သော External Storage Devices များထံသို့ ကူးစက်ကာ အခြားကွန်ပျူတာများထံသို့ ပျံ့နှံ့ရန် ကြိုးစားပါသည်။ PlugX သည် အင်တာနက်ချိတ်ဆက်မထားသော ကွန်ပျူတာများထံမှ သတင်းအချက်အလက်များကို ခိုးယူရန် အထူးဖန်တီးထားသော Remote Access Trojan ဖြစ်ပါသည်။



➤PlugX RAT တိုက်ခိုက်မှု မခံရရေးအတွက် အောက်ပါအတိုင်း လိုက်နာဆောင်ရွက်သင့်ပါသည်–

(က) မိမိမသိရှိသောသူများမှပေးပို့သော မည်သည့်ဖိုင်ကိုမဆို၊ Link များကိုမဆို မစစ်ဆေးဘဲ အလွယ်တကူဖွင့်မကြည့်ရန်။

(ခ) မိမိသိရှိသောသူမှ ပေးပို့သောမေးလ်ဖြစ်ခဲ့လျှင် မည်သည့်အကြောင်းကြောင့် ထိုမေးလ်ကို လက်ခံရရှိသည်ကို ဝေခွဲမရသည့်အခါတွင် ပေးပို့သူအား သေချာအောင်မေးမြန်းပြီးမှသာ မေးလ်အားဖွင့်ကြည့်ရန်။

(ဂ) မသင်္ကာဖွယ်မေးလ်များ လက်ခံရရှိပါက ထိုမေးလ်များအား အခြားသူများထံ Forward လုပ်ခြင်းများ မလုပ်ဘဲ mmCERT သို့ပေးပို့၍ တိုင်ကြားရန်။

(ဃ) မယုံကြည်ရသော Website များမှ ပရိုဂရမ်များ၊ ဖိုင်များ Download လုပ်ရာတွင် Virustotal (www.virustotal.com) ကဲ့သို့ Website များတွင် သေချာအောင် စစ်ဆေးပြီးမှ ဖွင့်ကြည့်ရန်။

(င) Microsoft Word ဖိုင်အဖြစ် ပေးပို့လာသောဖိုင်များအား Microsoft Word ဖိုင် ဟုတ်၊ မဟုတ် Notepad ဖြင့် စစ်ဆေးရန်။

(စ) Memory Stick ထဲရှိ ဖိုင်များကို ဖွင့်ရာတွင် ပရိုဂရမ်ဖိုင်များပါရှိပါက စစ်ဆေးပြီးမှသာ ဖွင့်ကြည့်ရန်။ Shortcut ဖိုင်များကို ဖွင့်မကြည့်ရန်။

(ဆ) မိမိတို့၏ Microsoft Windows၊ Microsoft Office ပရိုဂရမ်များနှင့် Anti-virus ပရိုဂရမ်များကို နောက်ဆုံးအခြေအနေအထိ Update ပြုလုပ်ပြီး Anti-virus အား မည်သည့်အကြောင်းကြောင်းဖြင့်မျှ မပိတ်ရန်။

mmCERT
MYANMAR COMPUTER EMERGENCY RESPONSE TEAM
Myanmar Computer Emergency Response Team