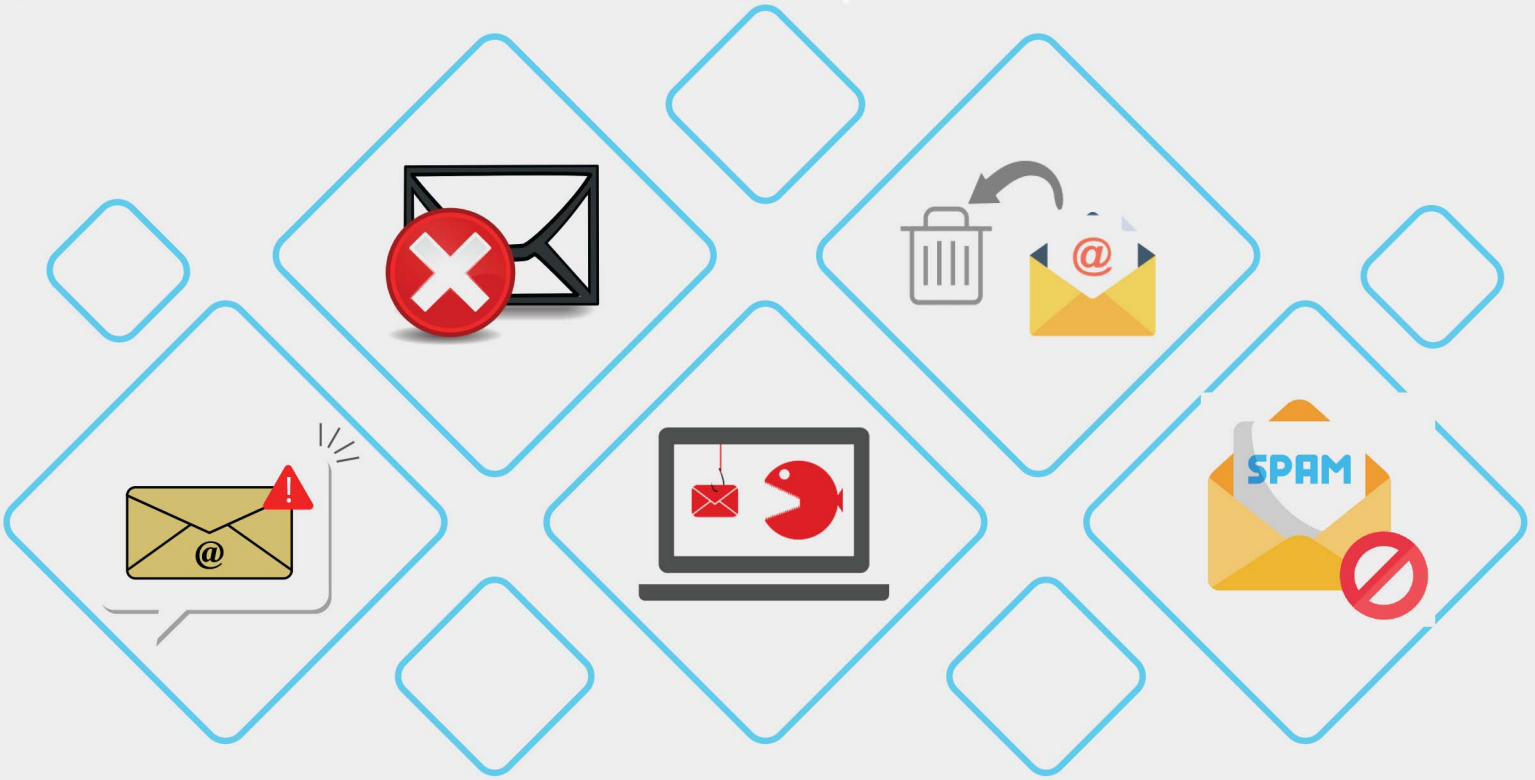
mmCERT
MYANMAR COMPUTER EMERGENCY RESPONSE TEAM



Guidebook for Suspicious Mails

Version 1.0

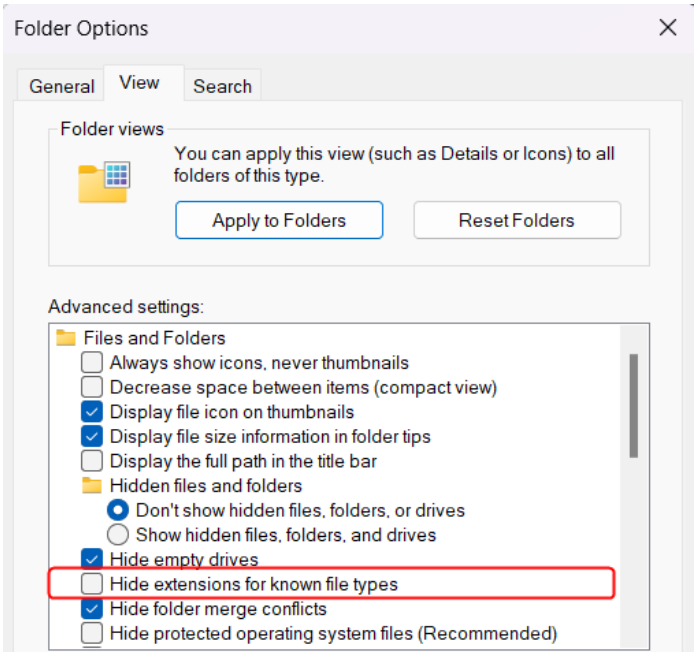
အန္တရာယ်ဖြစ်စေနိုင်သည့် အီးမေးလ်များ လက်ခံရရှိပါက လိုက်နာဆောင်ရွက်ရမည့်အချက်များ

၁။ အန္တရာယ်ဖြစ်စေနိုင်သည့် အီးမေးလ်ဆိုသည်မှာ မိမိမသိရှိသောသူထံမှ ပေးပို့သောအီးမေးလ်များ၊ မိမိ၏မိတ်ဆွေအယောင်ဆောင်၍ ပေးပို့သော အီးမေးလ်များ၊ မည်သည့်အကြောင်းကြောင့် မေးလ်အား လက်ခံရရှိသည်ကို မခွဲခြားနိုင်သော အီးမေးလ်များဖြစ်ပြီး အဆိုပါအီးမေးလ်များတွင် အဖျက်အမှောက် Link များ၊ ချုံ့ထားသော Zip ဖိုင်များနှင့် အဖျက်အမှောက်ကုဒ်များပါသော Microsoft Office ဖိုင်များ (Word ဖိုင်နှင့် Excel ဖိုင်များ) ပါဝင်တတ်ပါသည်။

၂။ အန္တရာယ်ဖြစ်စေနိုင်သည့် အီးမေးလ်များအား လက်ခံရရှိခြင်းမှ လျော့ကျစေရန်အတွက် ရုံးလုပ်ငန်းသုံးအီးမေးလ်လိပ်စာများကို ရုံးလုပ်ငန်းကိစ္စရပ်များ ပေးပို့ဆောင်ရွက်ခြင်းအတွက်သာ အသုံးပြုရန်ဖြစ်ပြီး ရုံးလုပ်ငန်းများနှင့် မသက်ဆိုင်သော လူမှုကွန်ရက်များ၊ ဖိုရမ်များနှင့် Website များတွင် အသုံးပြုခြင်းအား ရှောင်ကြဉ်ရပါမည်။ မိမိ၏အီးမေးလ်လိပ်စာအား မသက်ဆိုင်သူများထံ ပေးခြင်းနှင့် လူမှုကွန်ရက်များတွင် ဖော်ပြခြင်းအား ရှောင်ကြဉ်ရပါမည်။

၃။ အီးမေးလ်လိပ်စာများအား အလိုအလျောက် ရှာဖွေစုဆောင်းကာ အဖျက်အမှောက်မေးလ်များ ပေးပို့လျက်ရှိသော ပရိုဂရမ်များက မိမိ၏အီးမေးလ်လိပ်စာအား စုဆောင်းနိုင်ခြင်း မရှိစေရန်အတွက် ဌာနများ၏ Website များတွင် မဖြစ်မနေဖော်ပြရန်လိုသော အီးမေးလ်လိပ်စာများကိုသာ ဖော်ပြရန် လိုအပ်ပါသည်။

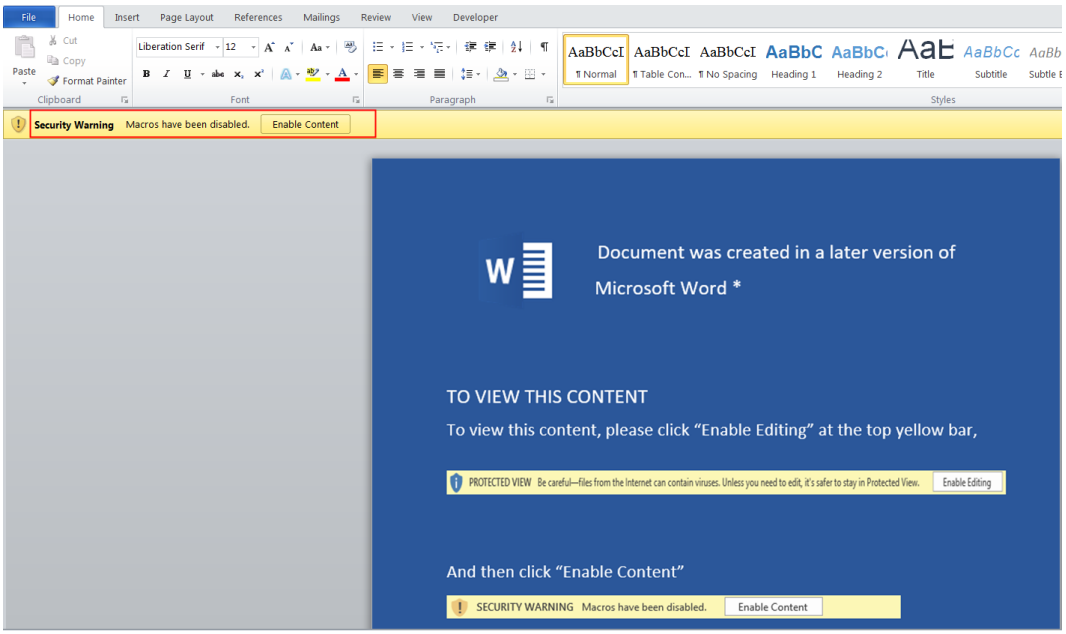
၄။ အီးမေးလ်များတွင် တွဲပါလေ့ရှိသော ဖိုင်များသည် Zip ဖိုင်အမျိုးအစားဖြစ်ပြီး အဆိုပါဖိုင်များအား ဖွင့်ရန် Password များအား အီးမေးလ်၏စာကိုယ်တွင် တစ်ပါတည်းရေးသားဖော်ပြထားပါက အဆိုပါ ဖိုင်သည် အဖျက်အမှောက်ကုဒ်များပါသောဖိုင် ဖြစ်နိုင်ခြေ များပါသည်။ ဟက်ကာများသည် ဆိုက်ဘာ လုံခြုံရေးစောင့်ကြည့်စနစ်များက ဖိုင်များကို စစ်ဆေးခြင်းမှ ရှောင်ရှားနိုင်ရန်အတွက် ဖိုင်များတွင် Password များကို သတ်မှတ်တတ်ကြပါသည်။ Zip ဖိုင်ထဲတွင် ပါရှိသောဖိုင်သည် .Exe ဖိုင်အမျိုးအစား (ပရိုဂရမ်ဖိုင်များ)နှင့် .Lnk ဖိုင်အမျိုးအစား (Shortcut ဖိုင်များ) ဖြစ်ပါက ၎င်းဖိုင်များအားလုံးသည် အဖျက်အမှောက်ဖိုင်များ ဖြစ်ကြပါသည်။ (ဖိုင်အမျိုးအစားများကို Microsoft Windows မှ ပြသပေးနိုင်အတွက် Windows Explorer ၏ Folder Option Setting တွင် “Hide Extensions for Known File Types” အား အမှန်ခြစ် ရွေးချယ် ထားခြင်းအား ဖြုတ်ထားရန် လိုအပ်ပါသည်။) အဆိုပါ အဖျက်အမှောက်ဖိုင်များကို ဖွင့်မိပါက ကွန်ပျူတာအား ပိတ်၍ CIO (Chief Information Officer) ထံသို့ ချက်ချင်း အကြောင်းကြားရန် လိုအပ်ပါသည်။



ပုံ(၁) - ဖိုင်အမျိုးအစားကို ဖော်ပြနိုင်ရန်အတွက် အမှန်ခြစ်အား ဖြုတ်ထားရန် လိုအပ်ပုံ

၅။ .Docm ဖိုင်အမျိုးအစား (Macro ကုဒ်များပါသော Word ဖိုင်များ)၊ .Xlsm ဖိုင်အမျိုးအစား (Macro ကုဒ်များပါသော Excel ဖိုင်များ)၊ .Js ဖိုင်အမျိုးအစား (JavaScript ဖိုင်များ)၊ .Html ဖိုင်အမျိုးအစား (HyperText Markup Language ဖိုင်များ) တို့သည် အဖျက်အမှောက်ကုဒ်များပါသော ဖိုင်များဖြစ်သည့် အတွက် အဆိုပါဖိုင်များကို ဖွင့်ကြည့်ခြင်း မပြုရပါ။

၆။ Microsoft Word ဖိုင်များနှင့် Excel ဖိုင်များ ဖွင့်ကြည့်သည့်အခါ “Security Warning” သတိပေးချက်အား မြင်တွေ့ရပါက အဆိုပါဖိုင်သည် အဖျက်အမှောက်ကုဒ်များပါရှိသည့် Microsoft Office ဖိုင် ဖြစ်ပါသည်။ “Enable Content” အားနှိပ်ပါက အဖျက်အမှောက်ကုဒ်များ အလုပ်လုပ်မည် ဖြစ်ပါသည်။



ပုံ(၂) - အဖျက်အမှောက်ကုဒ်များပါသော Microsoft Office ဖိုင်

၇။ အီးမေးလ်တွင်ပါလာသော .Rtf ဖိုင်အမျိုးအစား (Rich Text Format ဖိုင်)နှင့် .Pdf (Portable Document Format ဖိုင်)တို့ကို Update မဖြစ်တော့သည့် Microsoft Word နှင့် Adobe Acrobat Reader တို့ဖြင့် ဖွင့်ပါက အဖျက်အမှောက်ကုဒ်များကို အလုပ်လုပ်စေနိုင်မည်ဖြစ်သဖြင့် Microsoft Office 2019 နှင့် Adobe Acrobat Reader 11 ကဲ့သို့ Version မြင့်သောဆော့ဖ်ဝဲလ်များကို အသုံးပြုရန် လိုအပ်ပါသည်။

၈။ အန္တရာယ်ဖြစ်စေနိုင်သည့် အီးမေးလ်များ လက်ခံရရှိပါက အဆိုပါအီးမေးလ်အား ဖျက်ခြင်း၊ အခြားသူများထံသို့ ဆက်လက်ပေးပို့ခြင်းများ မပြုလုပ်ဘဲ မေးလ်တွင်ပါဝင်သော Link များ၊ တွဲပါလာသောဖိုင်များကို စစ်ဆေးနိုင်ရန်အတွက် အဆိုပါမေးလ်အား Junk Folder ထဲသို့ ပြောင်းရွှေ့သိမ်းဆည်းပြီး CIO ထံ သတင်းပို့ရပါမည်။

၉။ အီးမေးလ်တွင် ပါဝင်သော Link များနှင့် တွဲပါလာသောဖိုင်များကို ဖွင့်ကြည့်စဉ်အတွင်း မိမိ၏ ကွန်ပျူတာရှိ Antivirus ပရိုဂရမ်ကို ယာယီပိတ်ထားခြင်း လုံးဝ မပြုလုပ်ရပါ။ Antivirus ပရိုဂရမ်များအား နောက်ဆုံးအခြေအနေထိ Update ပြုလုပ်ထားရပါမည်။

၁၀။ အီးမေးလ်ဖတ်ရှုသော Web Browser (Firefox နှင့် Chrome စသည်) များတွင် User Name နှင့် Password များကို သိမ်းဆည်းထားခြင်း လုံးဝ မပြုလုပ်ရပါ။ အီးမေးလ်လိပ်စာနှင့် ပတ်သက်သော Password များကို အခြားသူများထံသို့ ဝေမျှခြင်း မပြုလုပ်ရပါ။

၁၁။ မိမိ၏အီးမေးလ်အား ဆိုက်ဘာတိုက်ခိုက်ခံထားရမှု ရှိ၊ မရှိအား သိရှိနိုင်ရန်အတွက် https://haveibeenpwned.com/ နှင့် https://www.haveibeenemotet.com/ တို့တွင် သွားရောက်စစ်ဆေးနိုင်ပါသည်။

၁၂။ ယနေ့ခေတ်တွင် အဖွဲ့အစည်းများ၊ ကုမ္ပဏီကြီးများတွင် ဆိုက်ဘာလုံခြုံရေးစနစ်များကို တပ်ဆင်လာကြသည့်အတွက် ဟက်ကာများ၏ အားနည်းမှုရှိသည့်ဝန်ထမ်းများကို အဓိက ပစ်မှတ်ထားတိုက်ခိုက်လာသည့်အတွက် ဝန်ထမ်းများအား Phishing နှင့်ပတ်သက်သည့် အသိပညာပေးသင်တန်းများ ပို့ချခြင်း၊ ရှောင်တခင် စမ်းသပ်စစ်ဆေးခြင်းများ ဆောင်ရွက်သွားရန် လိုအပ်ပါသည်။

၁၃။ ဆိုက်ဘာတိုက်ခိုက်ခံရမှုများနှင့်ပတ်သက်၍ တိုင်ကြားလိုပါကနှင့် အကြံပြုချက်များရယူလိုပါက ပို့ဆောင်ရေးနှင့်ဆက်သွယ်ရေးဝန်ကြီးဌာန၊ သတင်းအချက်အလက်နည်းပညာနှင့်ဆိုက်ဘာလုံခြုံရေးဦးစီးဌာန၊ အမျိုးသားဆိုက်ဘာလုံခြုံရေးဗဟိုဌာန၏ ဖုန်းနံပါတ်ဖြစ်သော ၀၆၇-၃၄၂၂၂၇၂ သို့ ဆက်သွယ်၍ ဖြစ်စေ၊ အီးမေးလ်များဖြစ်သော infoteam@mmcert.org.mm နှင့် incident@ncsc.gov.mm သို့ဖြစ်စေ ဆက်သွယ်တိုင်ကြားနိုင်ပါသည်။