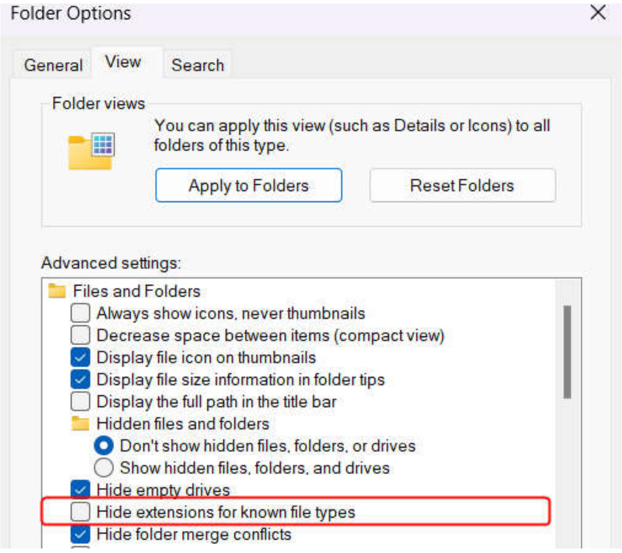
သံသယဖြစ်ဖွယ် အီးမေးလ်များ လက်ခံရရှိပါက လိုက်နာဆောင်ရွက်ရမည့် အချက်များ

၁။ သံသယဖြစ်ဖွယ် အီးမေးလ်ဆိုသည်မှာ မိမိမသိရှိသောသူထံမှ ပေးပို့သော အီးမေးလ်များ၊ မိမိ၏ မိတ်ဆွေအယောင်ဆောင်၍ ပေးပို့သော အီးမေးလ်များ၊ မည်သည့်အကြောင်းကြောင့် မေးလ်အား လက်ခံရရှိသည်ကို မခွဲခြားနိုင်သော အီးမေးလ်များဖြစ်ပြီး အဆိုပါအီးမေးလ်များတွင် အဖျက်အမှောင့် Link များ၊ ချုံ့ထားသော Zip ဖိုင်များနှင့် အဖျက်အမှောင့်ကုဒ်များပါသော Microsoft Office ဖိုင်များ (Word ဖိုင်နှင့် Excel ဖိုင်များ)ပါဝင်တတ်ပြီး Password ထားရှိ၍ အဆိုပါ Password အား စာကိုယ်တွင် ဖော်ပြထားလေ့ရှိပါသည်။

၂။ သံသယဖြစ်ဖွယ်အီးမေးလ်များအား လက်ခံရရှိခြင်းမှ လျော့ကျစေရန်အတွက် ရုံးလုပ်ငန်းသုံး အီးမေးလ်လိပ်စာများကို ရုံးလုပ်ငန်းကိစ္စရပ်များ ပေးပို့ဆောင်ရွက်ခြင်းအတွက်သာ အသုံးပြုရန်ဖြစ်ပြီး ရုံးလုပ်ငန်းများနှင့် မသက်ဆိုင်သော လူမှုကွန်ရက်များ၊ ဖိုရမ်များနှင့် Website များတွင် အသုံးပြုခြင်း အား ရှောင်ကြဉ်ရပါမည်။ မိမိ၏ အီးမေးလ်လိပ်စာအား မသက်ဆိုင်သူများထံ ပေးခြင်းနှင့် လူမှုကွန်ရက် များတွင် ဖော်ပြခြင်းအား ရှောင်ကြဉ်ရပါမည်။

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

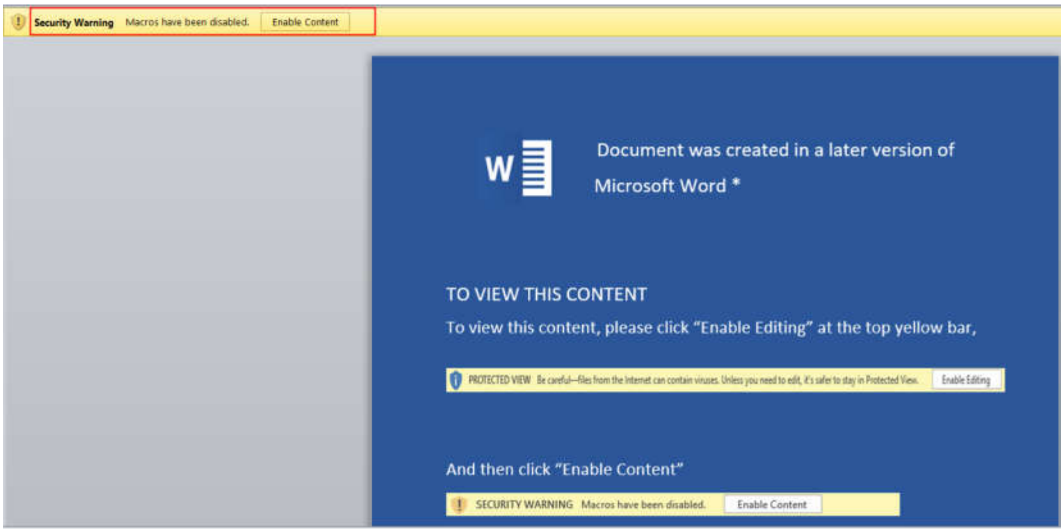
၄။ အီးမေးလ်များတွင် တွဲပါလေ့ရှိသော ဖိုင်များအား Password ဖြင့် သိမ်းဆည်းထားပြီး ၎င်းအား ဖွင့်ရန် Password ကို အီးမေးလ်၏ စာကိုယ်တွင် တစ်ပါတည်းရေးသားဖော်ပြထားပါက အဆိုပါ ဖိုင်သည် ဆိုက်ဘာလုံခြုံရေးစနစ်များက ဖိုင်များကို စစ်ဆေးခြင်းမှ ရှောင်ရှားနိုင်ရန်အတွက် Password ဖြင့် သိမ်းဆည်းခြင်းဖြစ်သောကြောင့် အဖျက်အမှောင့်ကုဒ်များပါသောဖိုင် ဖြစ်နိုင်ခြေများပါသည်။ တွဲပါလေ့ရှိသော Zip ဖိုင်ထဲတွင်ပါသည့် ဖိုင်များသည် .Exe ဖိုင်အမျိုးအစား (ပရိုဂရမ်ဖိုင်များ)နှင့် .Lnk ဖိုင်အမျိုးအစား (Shortcut ဖိုင်များ) ဖြစ်ပါက ၎င်းဖိုင်များအားလုံးသည် အဖျက်အမှောင့်ဖိုင်များ ဖြစ်ကြပါသည်။ (ဖိုင်အမျိုးအစားများကို Microsoft Windows မှ ပြသပေးနိုင် အတွက် Windows Explorer ၏ Folder Option Setting တွင် “Hide Extensions for Known File Types” အား အမှန်ခြစ် ရွေးချယ်ထားခြင်းအား ဖြုတ်ထားရန် လိုအပ်ပါသည်။)



ပုံ(၁) - ဖိုင်အမျိုးအစားကို ဖော်ပြနိုင်ရန်အတွက် အမှန်ခြစ်အား ဖြုတ်ထားရန် လိုအပ်ပုံ

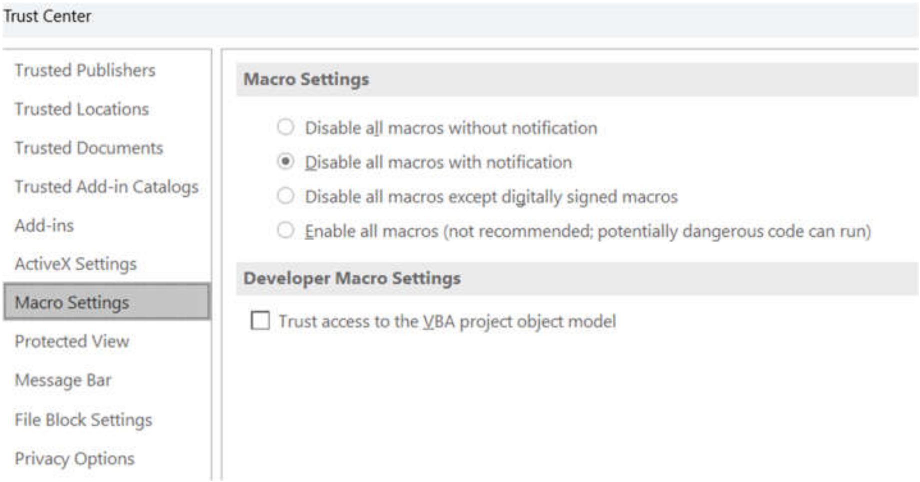
၅။ .Docm ဖိုင်အမျိုးအစား (Macro ကုဒ်များပါသော Word ဖိုင်များ)၊ .Xlsm ဖိုင်အမျိုးအစား (Macro ကုဒ်များပါသော Excel ဖိုင်များ)၊ .Js ဖိုင်အမျိုးအစား (JavaScript ဖိုင်များ)၊ .Html ဖိုင် အမျိုးအစား (HyperText Markup Language ဖိုင်များ) တို့သည် အဖျက်အမှောင့်ကုဒ်များပါသော ဖိုင်များ ဖြစ်သည့်အတွက် အဆိုပါဖိုင်များကို ဖွင့်ကြည့်ခြင်း မပြုရပါ။

၆။ Microsoft Word ဖိုင်များနှင့် Excel ဖိုင်များ ဖွင့်ကြည့်သည့်အခါ “Security Warning” သတိပေး ချက်အား မြင်တွေ့ရပါက အဆိုပါဖိုင်သည် အဖျက်အမှောင့်ကုဒ်များပါရှိသည့် Microsoft Office ဖိုင် ဖြစ်ပါသည်။ “Enable Content” အားနှိပ်ပါက အဖျက်အမှောင့်ကုဒ်များ အလုပ်လုပ်မည် ဖြစ်ပါသည်။



ပုံ(၂) - အဖျက်အမှောင့်ကုဒ်များပါသော Microsoft Office ဖိုင်

၇။ Macros ကုတ်များ အလိုအလျောက် အလုပ်လုပ်ခြင်းမဖြစ်စေရန်အတွက် Microsoft Word ၏ Option မှ Trust Center Setting တွင် Disable Macros ပြုလုပ်ထားသင့်ပါသည်။



ပုံ(၃) - ဖိုင်များရှိ Macro များ အလိုအလျောက်အလုပ်မလုပ်စေရန် Disable ထားပုံ

၈။ ဝန်ကြီးဌာနများအနေဖြင့် သံသယဖြစ်ဖွယ် အီးမေးလ်များ လက်ခံရရှိပါက အဆိုပါအီးမေးလ်အား ဖျက်ပစ်ခြင်း၊ အခြားသူများထံသို့ ဆက်လက်ပေးပို့ခြင်းများ မပြုလုပ်ဘဲ မေးလ်တွင်ပါဝင်သော Link များ၊ တွဲပါလာသော ဖိုင်များကို စစ်ဆေးနိုင်ရန်အတွက် အဆိုပါမေးလ်အား Junk Folder ထဲသို့ ပြောင်းရွှေ့သိမ်းဆည်းပြီး သက်ဆိုင်ရာ CIO ထံ သတင်းပို့ရပါမည်။

၉။ အဆိုပါသံသယဖြစ်ဖွယ်အီးမေးလ်ပါ ပူးတွဲဖိုင်များနှင့် Link များအား ဖွင့်ကြည့်ဝင်ရောက်မိပါက ကွန်ပျူတာအား ပိတ်၍ CIO (Chief Information Officer) ထံသို့ ချက်ချင်း အကြောင်းကြားရန် လိုအပ်ပါသည်။

၁၀။ သံသယဖြစ်ဖွယ်အီးမေးလ်အများစုတွင် Antivirus စသည့် ဆိုက်ဘာလုံခြုံရေးစနစ်များအား ရှောင်ရှားရန်အတွက် Attached File များအား Password ခံထားလေ့ရှိခြင်းနှင့် အဆိုပါ Password အား ပေးပို့ခံရသူမှ အလွယ်တကူသိရှိပြီး ဖွင့်ကြည့်နိုင်စေရန် စာကိုယ်တွင် ရေးသားဖော်ပြထားလေ့ရှိခြင်းတို့ကြောင့် ယင်းကဲ့သို့ Password ပူးတွဲပါသော အီးမေးလ်များ လက်ခံရရှိပါက ပေးပို့သူအား သေချာအတည်ပြုပြီးမှသာ ဖွင့်ကြည့်သင့်ပါသည်။

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

၁၂။ အီးမေးလ်ဖတ်ရှုသော Web Browser (Firefox နှင့် Chrome စသည်) များတွင် User Name နှင့် Password များကို သိမ်းဆည်းထားခြင်း လုံးဝ မပြုလုပ်ဘဲ Password Manager အား အသုံးပြုသင့်ပါသည်။ ခိုင်မာသော Password အား ထားရှိရန်နှင့် Password များကို အခြားသူများထံသို့ ဝေမျှခြင်း မပြုလုပ်ရန် လိုအပ်ပါသည်။

၁၃။ ယခုအခါ ကမ္ဘာတစ်ဝှမ်းတွင် ဆိုက်ဘာတိုက်ခိုက်မှုများ၊ သတင်းအချက်အလက် ပေါက်ကြားမှုများ၊ ကိုယ်ရေးအချက်အလက်ဖွင့်ချခြင်းများ မကြာခဏဖြစ်ပေါ်နေပါသဖြင့် အဆိုပါခြိမ်းခြောက်မှုများအား မပြတ်သိရှိစေရန်နှင့် အဆိုပါကိစ္စများဖြစ်ပေါ်လာပါက မိမိတို့၏ Password များကို အချိန်နှင့်တစ်ပြေးညီ ပြောင်းလဲသတ်မှတ်ကြရန် လိုအပ်ပါသည်။ မိမိ၏အီးမေးလ်အား သတင်းပေါက်ကြားမှု ရှိ၊ မရှိအား သိရှိနိုင်ရန်အတွက် https://haveibeenpwned.com တွင် သွားရောက်စစ်ဆေးနိုင်ပါသည်။

၁၄။ ဆိုက်ဘာလုံခြုံရေးကျိုးပေါက်မှုများကြောင့် အခါအားလျော်စွာ Product Vendor များမှ ပြင်ဆင်သော Patch များအား အချိန်မီ Update လုပ်ရန်နှင့် အသုံးပြုသော Software များ၊ Browser များနှင့် Antivirus များအား နောက်ဆုံးဗားရှင်းအား အသုံးပြုရန် လိုအပ်ပါသည်။

၁၅။ ယနေ့ခေတ်တွင် အစိုးရအဖွဲ့အစည်းများ၊ ကုမ္ပဏီကြီးများတွင် ဆိုက်ဘာလုံခြုံရေးစနစ်များကို တပ်ဆင်လာကြသဖြင့် ဆိုက်ဘာတိုက်ခိုက်သူများက ဆိုက်ဘာလုံခြုံရေးအသိပညာ အားနည်းမှုရှိသော ဝန်ထမ်းများကို အဓိကပစ်မှတ်ထား တိုက်ခိုက်လာသည့်အတွက် ဝန်ထမ်းများအား Phishing နှင့် ပတ်သက်သည့် အသိပညာပေးသင်တန်းများ ပို့ချခြင်း၊ ရှောင်တခင် စမ်းသပ်စစ်ဆေးခြင်းများ ဆောင်ရွက်သွားရန် လိုအပ်ပါသည်။

၁၆။ ဆိုက်ဘာတိုက်ခိုက်ခံရမှုများနှင့်ပတ်သက်၍ တိုင်ကြားလိုပါက ပို့ဆောင်ရေးနှင့်ဆက်သွယ်ရေးဝန်ကြီးဌာန၊ သတင်းအချက်အလက်နည်းပညာနှင့် ဆိုက်ဘာလုံခြုံရေးဦးစီးဌာန၊ မြန်မာဆိုက်ဘာအရေးပေါ်တုံ့ပြန်ရေးဌာနခွဲ (mmcert) ၏ ဖုန်းနံပါတ်ဖြစ်သော ၀၆၇-၃၄၂၂၂၇၂ သို့ ဆက်သွယ်၍ဖြစ်စေ၊ infoteam@mmcert.org.mm နှင့် incident@mmcert.org.mm သို့ဖြစ်စေ ဆက်သွယ်တိုင်ကြားပြီး အကြံပြုချက်များ ရယူနိုင်ပါသည်။