ပြည်သူ့လွှတ်တော်ရုံး
သူတေသနဌာန

ရက်စွဲ။ ၂၀၂၆ ခုနှစ်၊ မေလ ၂၁ ရက်

လူမှုကွန်ရက်အသုံးပြုသူတိုင်း သိထားသင့်သည့် ဆိုက်ဘာလုံခြုံရေး

အကျဉ်းချုပ်

ယနေ့ခေတ် နည်းပညာအရှိန်အဟုန်ဖြင့် ဖွံ့ဖြိုးတိုးတက်လာသော ဒီဂျစ်တယ်ခေတ်တွင် ဆိုက်ဘာလုံခြုံရေးသည် နိုင်ငံတော်၏လုံခြုံရေးနှင့် လူတစ်ဦးချင်းစီ၏ လူမှုစီးပွားဘဝများအတွက် မရှိမဖြစ်လိုအပ်သော အခြေခံအုတ်မြစ်တစ်ခု ဖြစ်ပါသည်။ နေ့စဉ်လူမှုဘဝတွင် အင်တာနက်နှင့် နည်းပညာအပေါ် မှီခိုမှုမြင့်မားလာသည်နှင့်အမျှ အရေးကြီးအချက်အလက်များကိုတိုက်ခိုက်ခြင်း၊ ဖျက်ဆီးခြင်းနှင့် ခွင့်ပြုချက်မရှိဘဲ ဝင်ရောက်ရယူခြင်းစသည့် ဆိုက်ဘာခြိမ်းခြောက်မှုများသည် ကြီးမားသော စိန်ခေါ်မှုတစ်ရပ် ဖြစ်လာပါသည်။ ဆိုက်ဘာလုံခြုံရေးသည် နည်းပညာဆိုင်ရာ ကာကွယ်မှုသက်သက်သာမကဘဲ အစိုးရ၊ ပြည်သူနှင့် ပုဂ္ဂလိကကဏ္ဍတို့၏ ပုံရိပ်၊ အရင်းအမြစ်များနှင့် အရေးကြီးသော ဝန်ဆောင်မှုများကို လုံခြုံစွာ လည်ပတ်နိုင်စေရန် ပံ့ပိုးပေးသည့် အဓိကကဏ္ဍတစ်ခု ဖြစ်ပါသည်။

ဤစာတမ်းတိုတွင် လူမှုကွန်ရက်အသုံးပြုသူများ သတိပြုသင့်သည့် ဖြစ်ပွားမှုများသော ဆိုက်ဘာတိုက်ခိုက်မှုအမျိုးအစားများ၊ ဆိုက်ဘာလုံခြုံရေးအတွက် လိုက်နာရမည့်အခြေခံအချက်များ၊ ဉာဏ်ရည်တုနည်းပညာ(AI)နှင့်ဆိုက်ဘာလုံခြုံရေး၊ ဆိုက်ဘာလုံခြုံရေးဥပဒေပါပြဋ္ဌာန်းချက်များ၊ ကမ္ဘာတွင် မြန်မာနိုင်ငံ၏ဆိုက်ဘာလုံခြုံရေးအဆင့်များကို လေ့လာ၍ ရေးသားပြုစု တင်ပြထားပါသည်။

သုတေသနစာတမ်းတိုအမှတ်စဉ် (၃၃၄)

မာတိကာ

နိဒါန်း

၁။ သတင်းအချက်အလက်နှင့် ဆက်သွယ်ရေးနည်းပညာ (ICT)ကဏ္ဍ ဖွံ့ဖြိုးတိုးတက်လာသည်နှင့်အညီ ဆိုက်ဘာလုံခြုံရေးသည် အရေးပါသော ကဏ္ဍတစ်ရပ် ဖြစ်လာပါသည်။ ဆိုက်ဘာလုံခြုံရေးဆိုသည်မှာ နည်းပညာ လုပ်ငန်းစဉ်နှင့် ကွန်ယက်များကို တိုက်ခိုက်ခြင်း၊ ဖျက်ဆီးခြင်း သို့မဟုတ် ခွင့်ပြုချက်မရဘဲ ဝင်ရောက်ရယူခြင်းမှ ကာကွယ်စောင့်ရှောက်ရန် ဒီဇိုင်းရေးဆွဲထားသော ပြုလုပ်ဆောင်ရွက်ချက်များ၊ စက်ကိရိယာများ၊ ပရိဂရမ်များနှင့် အချက်အလက်များကို ဆိုလိုပါသည်။ ဆိုက်ဘာလုံခြုံရေးသည် နည်းပညာဆိုင်ရာ သတင်းအချက်အလက်များ၏ လုံခြုံရေးလည်း ဖြစ်ပါသည်။

၂။ ဆိုက်ဘာလုံခြုံရေးသည် အစိုးရအဖွဲ့အစည်းများ၏ ပူးပေါင်းဆောင်ရွက်ရေးလုပ်ငန်းများ၊ အခြားအရေးပါသော လုပ်ငန်းစဉ်များ၊ အဖွဲ့အစည်းများမှ ကွန်ပျူတာနှင့် အခြားသောစက်ကိရိယာများတွင် အရေးကြီးသောသတင်းအချက်အလက်များကို လုံခြုံစွာ စုဆောင်းသိမ်းဆည်းနိုင်ရေးအတွက် အဓိကလုပ်ငန်းတစ်ရပ်ဖြစ်ပါသည်။ ဆိုက်ဘာတိုက်ခိုက်မှုများကြောင့် သတင်းအချက်အလက်စနစ်များကို ထိခိုက်နိုင်သည့်အပြင် အစိုးရ၊ ပြည်သူနှင့် ပုဂ္ဂလိကကဏ္ဍ အရင်းအမြစ်များနှင့် ဝန်ဆောင်မှုများ၏ပုံရိပ်များကိုပါ ထိခိုက်စေနိုင်ပါသည်။[1] ထို့ကြောင့် ဆိုက်ဘာလုံခြုံရေးသည် နည်းပညာပိုင်းဆိုင်ရာ ကာကွယ်မှုသက်သက်သာမကဘဲ အစိုးရ၊ ပြည်သူနှင့် ပုဂ္ဂလိကကဏ္ဍတို့၏ ပုံရိပ်၊ အရင်းအမြစ်များနှင့် အရေးကြီးသောဝန်ဆောင်မှုများကို လုံခြုံစွာ လည်ပတ်နိုင်စေရန် ပံ့ပိုးပေးသည့် အခြေခံအုတ်မြစ်တစ်ခု ဖြစ်လာပါသည်။

ရည်ရွယ်ချက်

၃။ ဤစာတမ်းတို့၏ရည်ရွယ်ချက်မှာ အောက်ပါအတိုင်းဖြစ်ပါသည်-

(က) ယနေ့ခေတ် နည်းပညာအသုံးပြုမှု မြင့်မားလာသည်နှင့်အမျှ လူမှုကွန်ရက်အသုံးပြုသူများအနေဖြင့် အဖြစ်များသော ဆိုက်ဘာတိုက်ခိုက်မှု အမျိုးအစားများနှင့် ၎င်းတို့၏ အန္တရာယ်များကို ခွဲခြားသိမြင်နိုင်စေရန်၊

(ခ) ဆိုက်ဘာတိုက်ခိုက်မှုများမှ ကာကွယ်နိုင်ရန်အတွက် လိုက်နာဆောင်ရွက်သင့်သည့်အခြေခံလုံခြုံရေးဆိုင်ရာ ကာကွယ်မှုနည်းလမ်းကောင်းများကို မျှဝေပေးရန်နှင့်

(ဂ) ၂၀၂၅ ခုနှစ်၊ ဆိုက်ဘာလုံခြုံရေးဥပဒေပါ ပြဋ္ဌာန်းချက်များကို သိရှိနားလည်ပြီး ဆိုက်ဘာအရင်းအမြစ်များကို စနစ်တကျနှင့် လုံခြုံစိတ်ချစွာ အသုံးပြုနိုင်စေရန်။

---

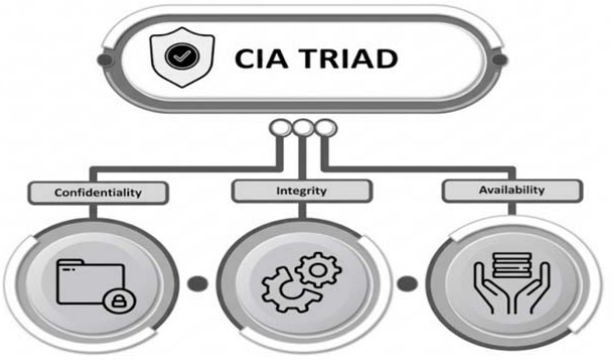
[1] ဒေါ်ချမ်းမြေ့ကြည်ကြည်ဇင်၊ ဥပဒေရေးရာဝန်ကြီးဌာန၊ ၁၆.၆.၂၀၂၃၊ https://www.mola.gov.mm/wp-content/uploads/2023/07/Weekly-News-15.pdf မှကောက်နုတ်ထားပါသည်။ (ကြည့်ရှုရရှိသည့်ရက် ၂၀၂၅ ခုနှစ်၊ ဒီဇင်ဘာလ ၁၅ ရက်)

သုတေသနနည်းနာနိသယများ

၄။ ဤစာတမ်းတိုတွင် ပြန်ကြားရေးဝန်ကြီးဌာနမှ ထုတ်ပြန်ထားသော သတင်းအချက်အလက်များ၊ မြန်မာဥပဒေသတင်းအချက်အလက်စနစ်၊ Myanmar National Portal နှင့် Cybersecurity & Infrastructure Security Agency တို့မှရရှိသော သတင်းအချက်အလက်များကို ပြုစုလေ့လာ၍ ကောက်နုတ် တင်ပြထားခြင်း ဖြစ်ပါသည်။

ဆိုက်ဘာလုံခြုံရေး၏ အဓိကမဏ္ဍိုင်(၃)ရပ် (CIA Triad)

၅။ ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာစနစ်များကို အဓိကမဏ္ဍိုင်ကြီး(၃)ရပ်ဖြစ်သော လျှို့ဝှက်ထားနိုင်မှု၊ မှန်ကန်တိကျမှုနှင့် အမြဲရရှိနိုင်မှု (CIA Triad) ပေါ်တွင် အခြေခံ၍ တည်ဆောက်ထားပါသည်။[2] အဆိုပါ CIA Triad သည် လုံခြုံရေးဆိုင်ရာ မူဝါဒများ (Security Policies) ချမှတ်ခြင်း၊ ဘေးအန္တရာယ်ဆန်းစစ်ချက်များ (Risk Assessments) ပြုလုပ်ခြင်းနှင့် လုံခြုံရေးဆိုင်ရာ မဟာဗျူဟာများ(Security Strategies) ကိုဖော်ဆောင်ရန် လမ်းညွှန်သည့် မူဘောင်တစ်ခုဖြစ်ပါသည်။[3] ထို့ကြောင့် ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ စနစ်တစ်ခုတည်ဆောက်ရာတွင် ခွင့်ပြုချက်ရှိသူများသာ သတင်းအချက်အလက်ကို ကြည့်ရှုခွင့်ရရှိအောင် ကန့်သတ်ထိန်းချုပ်သည့် လျှို့ဝှက်ထားနိုင်မှု (Confidentiality) လိုအပ်ပါသည်။ သတင်းအချက်အလက်များကို ခွင့်ပြုချက်မရှိဘဲ ပြင်ဆင်ခြင်း သို့မဟုတ် ဖျက်ဆီးခြင်းမှ တိတိကျကျ မှန်မှန်ကန်ကန် ကာကွယ်ပေးနိုင်မှု (Integrity)ရှိရမည် ဖြစ်ပါသည်။ ခွင့်ပြုချက်ရရှိသော အသုံးပြုသူများသာ မိမိတို့၏သတင်းအချက်အလက်များကို လိုအပ်သည့် အချိန်တိုင်း စိတ်ချယုံကြည်စွာအသုံးပြုနိုင်စေရန် ကာကွယ်ထားသည့် အမြဲရရှိနိုင်မှု (Availability) ဖြစ်ရပါမည်။ ဤအချက် (၃)ချက်ကို အခြေခံ၍ ဆိုက်ဘာလုံခြုံရေးစနစ်တစ်ခုကို တည်ဆောက်ရပါသည်။[4]



Source: SailPoint

[2] threatcop,May 17, 2025,https://threatcop.com/blog/three-goals-of-cybersecurity/ မှကောက်နုတ်ထားပါသည်။ (ကြည့်ရှုရရှိသည့်ရက် ၂၀၂၅ ခုနှစ်၊ ဒီဇင်ဘာလ ၂၀ ရက်)

[3] BITSIGHT,April 03, 2025, https://www.bitsight.com/glossary/cia-triad မှကောက်နုတ်ထားပါသည်။ (ကြည့်ရှုရရှိသည့်ရက် ၂၀၂၅ ခုနှစ်၊ ဒီဇင်ဘာလ ၂၅ ရက်)

[4] SailPoint ,January 16, 2025,CIA triad: Confidentiality, integrity, and availability မှကောက်နုတ်ထားပါသည်။ (ကြည့်ရှုရရှိသည့်ရက် ၂၀၂၅ ခုနှစ်၊ ဒီဇင်ဘာလ ၂၈ ရက်)

ခေတ်သစ်ကမ္ဘာတွင် ဆိုက်ဘာလုံခြုံရေး၏ အရေးပါမှု

၆။ ကမ္ဘာတစ်ဝန်းတွင် ဆိုက်ဘာလုံခြုံရေးကဏ္ဍကို အမျိုးသားလုံခြုံရေး၏ အစိတ်အပိုင်း တစ်ရပ်အဖြစ်သတ်မှတ်၍ အလေးထား ဆောင်ရွက်လာကြပြီ ဖြစ်ပါသည်။ ပြည်သူပိုင်ကဏ္ဍနှင့် ပုဂ္ဂလိကပိုင်ကဏ္ဍနှစ်ရပ်လုံးရှိ စီးပွားရေးလုပ်ငန်းများ၊ လူမှုရေးလုပ်ငန်းများ၊ ဝန်ဆောင်မှုလုပ်ငန်း များစသည်တို့ကို ဆိုက်ဘာကမ္ဘာပေါ်တွင် တစ်နေ့တခြား တိုးမြှင့်အခြေပြုတည်ဆောက်နေကြပြီ ဖြစ်ပါသည်။ သို့ဖြစ်၍ဆိုက်ဘာလုံခြုံရေးသည် သာမန်ကဏ္ဍတစ်ခု မဟုတ်တော့ဘဲ နိုင်ငံတော်နှင့် နိုင်ငံသားများ၏ အကျိုးစီးပွားနှင့် တိုက်ရိုက်ဆက်စပ်နေသည့် အမျိုးသားလုံခြုံရေး ကဏ္ဍတစ်ရပ် ဖြစ်လာပါသည်။

၇။ နည်းပညာဖွံ့ဖြိုးမှုနှင့်အတူ နိုင်ငံများ၏ အမျိုးသား အကျိုးစီးပွားသည် ပြင်ပကမ္ဘာထက် Virtual World ဖြစ်သော ဆိုက်ဘာကမ္ဘာပေါ်သို့ ပြောင်းရွှေ့တည်ရှိလာနေပြီဖြစ်ရာ ပြိုင်ဘက် နိုင်ငံများ၊ အဖွဲ့အစည်းများ၏ ဦးတည်တိုက်ခိုက်လာမည့်အန္တရာယ်မှ ကောင်းစွာကာကွယ်နိုင်ရန် ပြင်ဆင်ရန်လိုအပ်လာပါသည်။ အနာဂတ်တွင် နိုင်ငံများအကြား စစ်ဆင်မှုများသည် သမားရိုးကျ စစ်ဆင်မှုများနှင့်အတူ ဆိုက်ဘာစစ်ဆင်မှုများကိုပါ ပေါင်းစပ်ကျင့်သုံး၍ တိုက်ခိုက်လာနိုင်ဖွယ် ရှိကြောင်း ပညာရှင်များက သုံးသပ်ထားကြပါသည်။ သို့ဖြစ်၍ အချို့သောနိုင်ငံများရှိ တပ်မတော် ဖွဲ့စည်းပုံတွင် ဆိုက်ဘာတပ်ဖွဲ့များကို ဖွဲ့စည်းကာ ဆိုက်ဘာတိုက်ခိုက်မှုမှ ခုခံကာကွယ်နိုင်ရေး အတွက် ပြင်ဆင်ဆောင်ရွက်လျက်ရှိနေကြသည်ကို တွေ့ရှိရပါသည်။[5]

ဖြစ်ပွားမှုများသော ဆိုက်ဘာတိုက်ခိုက်မှုအမျိုးအစားများ

၈။ ဖြစ်ပွားမှုများသော ဆိုက်ဘာတိုက်ခိုက်မှုအမျိုးအစားများမှာ အောက်ပါအတိုင်း ဖြစ်ပါသည်-

(က) **မောလ်ဝဲရ် (Malware)**။ မောလ်ဝဲရ် (Malware) ဆိုသည်မှာ ဆိုက်ဘာအရင်း အမြစ်အား အနှောင့်အယှက်ဖြစ်စေသော သို့မဟုတ် အန္တရာယ်ဖြစ်စေသော အဖျက်အမှောင့်ကုဒ်သင်္ကေတ (Malicious Code)ကို ဆိုသည်။[6] ကွန်ပျူတာစနစ် များကို နှောင့်ယှက်ဖျက်ဆီးရန်၊ ခွင့်ပြုချက်မရှိဘဲ အချက်အလက်များကို ခိုးယူရန် သို့မဟုတ် အဝေးမှ စောင့်ကြည့်ရန် ရည်ရွယ်ချက်ဖြင့် အသုံးပြုကြသည်။ ၎င်းတွင် ထရိုဂျန် (Trojan)၊ အဒ်ဝဲ (Adware)၊ စပိုင်ဝဲ (Spyware)နှင့် ရန်ဆန်ဝဲရ် (Ransomware) စသည်တို့ ပါဝင်သည်။

---

[5] တည်ကြည်မောင်၊ e-Governmentနှင့်ဆိုက်ဘာလုံခြုံရေး၊ MYANMAR NATIONAL PORTAL၊ https://shorturl.at/uz3N8 မှကောက်နုတ်ထားပါသည်။ (ကြည့်ရှုရရှိသည့်ရက် ၂၀၂၆ ခုနှစ်၊ ဧန်နဝါရီလ ၁၅ ရက်)

[6] မြန်မာဥပဒေသတင်းအချက်အလက်စနစ်၊ ဆိုက်ဘာလုံခြုံရေးဥပဒေ (နိုင်ငံတော်စီမံအုပ်ချုပ်ရေးကောင်စီဥပဒေအမှတ် ၁/၂၀၂၅)၊https://www.mlis.gov.mm/mLsView.do%3Bjsessionid=9F3834AD02CEABDE5DD44B9441050172?lawordSn=21662 မှကောက်နုတ်ထားပါသည်။ (ကြည့်ရှုရရှိသည့်ရက် ၂၀၂၆ ခုနှစ်၊ ဧန်နဝါရီလ ၂၁ ရက်)

(ခ) **ဖစ်ရှင်း(Phishing)**။ ဖစ်ရှင်း(Phishing)ဆိုသည်မှာ ယုံကြည်ရသည့် လူပုဂ္ဂိုလ် သို့မဟုတ် အဖွဲ့အစည်း (ဥပမာ– ဘဏ်၊ Google၊ Amazon) အဖြစ် ဟန်ဆောင်ကာ အီးမေးလ်၊ ဖုန်းစာတို သို့မဟုတ် လူမှုကွန်ရက်များမှတစ်ဆင့် အရေးကြီးအချက်အလက်များကို လိမ်လည်တောင်းယူခြင်းဖြစ်ပါသည်။ ၂၀၂၆ ခုနှစ်တွင် **Generative AI** ကို အသုံးပြု၍ လူတစ်ဦးချင်းစီ၏ လေသံ၊ ပုံစံတို့ကို အတုယူကာ ပိုမိုခေတ်မီစွာ လိမ်လည်တိုက်ခိုက်လာကြပါသည်။

(ဂ) **Man–in–the–middle (MITM)** ။ Man–in–the–middle(MITM) ဆိုသည်မှာ ဆက်သွယ်ပြောဆိုနေသူနှစ်ဦးကြားတွင် တိုက်ခိုက်သူက ကြားဖြတ်ဝင်ရောက်ပြီး အချက်အလက်များကို ခိုးယူခြင်း(သို့မဟုတ်) ပြုပြင်ပြောင်းလဲသည့် တိုက်ခိုက်မှုမျိုးဖြစ်ပါသည်။

(ဃ) **Distributed denial of Service (DDoS)**။ Distributed Denial of Service (DDoS) ဆိုသည်မှာ ကမ္ဘာအနှံ့ရှိ ဗိုင်းရပ်စ်ကူးစက်ခံထားရသော ကွန်ပျူတာအမြောက်အမြားမှတစ်ဆင့် ၎င်းစနစ်အတွင်းသို့ အချက်အလက် (Traffic) များအလွန်အကျွံပေးပို့တိုက်ခိုက်ခြင်းဖြစ်သည်။ ယင်းသို့လုပ်ဆောင်ခြင်းဖြင့် ဝက်ဘ်ဆိုက်သို့မဟုတ် စနစ်တစ်ခုအား ဝန်ပိသွားစေကာ ပုံမှန်အလုပ်လုပ်ဆောင်နိုင်ခြင်း မရှိတော့ဘဲ တရားဝင်အသုံးပြုသူများ ဝင်ရောက်ခွင့် ပြတ်တောက်သွားစေပါသည်။

(င) **Injection**။ Injection ဆိုသည်မှာ စနစ်တစ်ခုအတွင်းရှိ အားနည်းချက် (Vulnerabilities)များကိုအသုံးချကာ အန္တရာယ်ရှိသောကုဒ် (Code)များ ထည့်သွင်းပြီးအရေးကြီးသောအချက်အလက်များကို ရယူနိုင်ခြင်း၊ command များကို အဝေးမှလုပ်ဆောင်နိုင်ခြင်း သို့မဟုတ် စနစ်တစ်ခုကို ပြုပြင်မွမ်းမံနိုင်ခြင်းတို့ကို ပြုလုပ်နိုင်သည့်အတွက် ယနေ့ခေတ်ဆိုက်ဘာလုံခြုံရေးနယ်ပယ်တွင် ကြီးမားသောခြိမ်းခြောက်မှုတစ်ခုအဖြစ် ရပ်တည်လျက်ရှိပါသည်။[7]

[7] Coursera Staff , 5 Cybersecurity Threats to Know in 2026,Dec 5, 2025,https://www.coursera.org/articles/cybersecurity-threats မှကောက်နုတ်ထားပါသည်။ (ကြည့်ရှုရရှိသည့်ရက် ၂၀၂၅ ခုနှစ်၊ ဒီဇင်ဘာလ ၁၇ ရက်)

ဆိုက်ဘာလုံခြုံရေးအတွက် လိုက်နာရမည့် အခြေခံအချက်များ

၉။ ယနေ့ခေတ် ဒီဂျစ်တယ်လူနေမှုစနစ်တွင် လူမှုစီးပွားလုပ်ဆောင်ချက်များအားလုံးသည် အင်တာနက်နှင့် နည်းပညာအပေါ်တွင် များစွာမှီခိုလာရသည့်အတွက် အချက်အလက်ခိုးယူခြင်း နှင့်လိမ်လည်ခြင်းကဲ့သို့သော ဆိုက်ဘာတိုက်ခိုက်မှုများ ခံရနိုင်ခြေများသဖြင့် ဆိုက်ဘာလုံခြုံရေး ဆိုင်ရာ အလေ့အကျင့်ကောင်းများအား စနစ်တကျ လိုက်နာကျင့်သုံးရန် လိုအပ်ပါသည်။[8]

၁၀။ ထို့ကြောင့် လူပုဂ္ဂိုလ်နှင့်အဖွဲ့အစည်းများ၏အချက်အလက်များကို ဆိုက်ဘာတိုက်ခိုက်မှု များမှကာကွယ်နိုင်ရန်အတွက် အောက်ပါ အခြေခံအချက်များကို မဖြစ်မနေ လိုက်နာဆောင်ရွက် သင့်ပါသည်-

(က) ခန့်မှန်းရခက်ခဲသော ခိုင်မာသည့် စကားဝှက်များကို အသုံးပြုခြင်း၊

(ခ) စကားဝှက်အပြင် နောက်ထပ် အဆင့်ဆင့်အတည်ပြုခြင်းစနစ် (Multi-Factor Authentication) ကို ထည့်သွင်းခြင်း၊

(ဂ) ဆော့ဖ်ဝဲလ်များကို ပုံမှန် Update ပြုလုပ်ခြင်းနှင့်

(ဃ) အချက်အလက်ခိုးယူရန် ကြိုးပမ်းသည့် သံသယဖြစ်ဖွယ် Link များနှိပ်မိခြင်းမှ သတိထားရှောင်ကြဉ်ခြင်း။[9]

Source: Cybersecurity & Infrastructure Security Agency

[8] Homeland Security, October 18, 2013 ,Cybersecurity: A Shared Responsibility | Homeland Security မှကောက်နုတ်ထားပါသည်။ (ကြည့်ရှုရရှိသည့်ရက် ၂၀၂၆ ခုနှစ်၊ ဧန်နဝါရီလ ၁၀ ရက်)

[9] Cybersecurity & Infrastructure Security Agency,https://www.cisa.gov/topics/cybersecurity-best-practices မှကောက်နုတ်ထားပါသည်။ (ကြည့်ရှုရရှိသည့်ရက် ၂၀၂၆ ခုနှစ်၊ ဧန်နဝါရီလ ၇ ရက်)

ဉာဏ်ရည်တုနည်းပညာ(AI)နှင့် ဆိုက်ဘာလုံခြုံရေး

၁၁။ ကမ္ဘာပေါ်တွင် ဆက်သွယ်ရေးနည်းပညာများ အရှိန်အဟုန်ဖြင့် တစ်နေ့တခြား ဖွံ့ဖြိုးတိုးတက်လာရာ အခြေခံလူမှုဘဝဝန်ဆောင်မှုများမှ အာကာသပညာရပ်များအထိ အသုံးတွင်ကျယ်လာခဲ့ပါသည်။ အွန်လိုင်းနည်းပညာများ၊ ဒီဂျစ်တယ်စီမံခန့်ခွဲမှုစနစ်များ စသည်တို့သည် နိုင်ငံရေး၊ စီးပွားရေး၊ လူမှုရေး၊ စစ်ရေးကဏ္ဍများတွင် ကျယ်ပြန့်စွာဖြစ်ထွန်းလာပါသည်။ ဆက်သွယ်ရေးနည်းပညာများ အရှိန်အဟုန်ဖြင့် ဖွံ့ဖြိုးတိုးတက်လာမှုသည် ကောင်းကျိုးနှင့်အတူ ဆိုးကျိုးများလည်း ယှဉ်တွဲလိုက်ပါလာသည်ကို တွေ့ရှိရပါသည်။

၁၂။ ယခုအခါ ဒီဂျစ်တယ်နည်းပညာများထက် ပိုမိုအသုံးတွင်ကျယ်လာသည့် ဉာဏ်ရည်တုနည်းပညာ(AI)ပေါ်ပေါက်လာပါသည်။ ဉာဏ်ရည်တု (Artificial intelligence – AI) ဆိုသည်မှာ အသိဉာဏ်ရှိသောကိုယ်စားလှယ်များကို ဒီဇိုင်းထုတ်လေ့လာရန် သို့မဟုတ် စက်ကိရိယာတို့၏ အသိဉာဏ်ကိုဖန်တီးထားခြင်း ဖြစ်ပါသည်။ သိပ္ပံနှင့်နည်းပညာ မြင့်မားတိုးတက်လာသော လူ့အသိုက်အဝန်းတွင် AI နည်းပညာသည် ဆန်းသစ်သည့်ဝန်ဆောင်မှုများကို ပေးစွမ်းနိုင်ပါသည်။ အသိဉာဏ်အပြင် လူ့စိတ်ခံစားချက်ကိုနားလည်ခြင်း၊ ဆုံးဖြတ်ချက်ချမှတ်ခြင်းတို့ကို ထည့်သွင်း စဉ်းစားနိုင်စွမ်းရှိသည့် ဉာဏ်ရည်ထည့်သွင်းထားသော ဉာဏ်ရည်တု လူသားမိတ္တူတစ်မျိုး ဖြစ်ပါသည်။ မကြာသေးမီက ကမ္ဘာ့နိုင်ငံခေါင်းဆောင်များ၊ သိပ္ပံပညာရှင်များနှင့် နည်းပညာရှင်များသည် ဉာဏ်ရည်တုနည်းပညာ (AI)၏ အသုံးဝင်မှုများကိုသာမက ယင်းနည်းပညာကြောင့် ဖြစ်လာနိုင်သောအန္တရာယ်များအား သတိပြုနိုင်ရန်နှင့် ကာကွယ်နိုင်မည့် ဥပဒေများကိုပါ ဆုံးဖြတ်ပြဋ္ဌာန်းလာကြသည်ကိုတွေ့ရပါသည်။

၁၃။ ဉာဏ်ရည်တုနည်းပညာသည် လက်ရှိတွင် အဆင့်အမြင့်ဆုံးနည်းပညာတစ်ခုဖြစ်ပြီး လူသားတို့၏လူနေမှုဘဝကို တိုးတက်ကောင်းမွန်အောင် ဖန်တီးပေးနိုင်စွမ်းရှိသော်လည်း တစ်ချိန်တည်းမှာပင် အဆိုပါနည်းပညာကြောင့် လုံခြုံရေးခြိမ်းခြောက်မှုများ၊ အစိုးရအပေါ် ပြည်သူများ၏ ယုံကြည်မှုများထိခိုက်လာနိုင်သည်ဟု ပြောကြားချက်များရှိပါသည်။ ဉာဏ်ရည်တုနည်းပညာကြောင့် ပညာရေး၊ ကျန်းမာရေးကဏ္ဍများတွင် တိုးတက်ဖွံ့ဖြိုးမှုများရှိလာသလို လူတို့၏ကိုယ်စိတ်ကျန်းမာရေးကို ထိခိုက်စေနိုင်ခြင်း၊ သတင်းတု၊ သတင်းမှားများဖန်တီးနိုင်ခြင်း၊ အလုပ်အကိုင်များ ဆုံးရှုံးနိုင်ခြင်း၊ အနာဂတ်တွင် အဆိုပါနည်းပညာကြောင့်ပင် လူသားမျိုးနွယ်တစ်ခုလုံးကို အန္တရာယ်ပေးလာနိုင်ကြောင်း သုံးသပ်မှုများရှိပါသည်။

၁၄။ မြန်မာနိုင်ငံသည် ၂၀၁၃ ခုနှစ်တွင် ဆက်သွယ်ရေးဥပဒေကိုပြဋ္ဌာန်းပြီးနောက် ဆက်သွယ်ရေးနည်းပညာကဏ္ဍကို လွတ်လပ်သောစျေးကွက်အဖြစ် ဖွင့်လှစ်ပေးနိုင်မှုနှင့်အတူ နည်းပညာများ

အတိုင်းအတာတစ်ခုအထိ ဖွံ့ဖြိုးတိုးတက်လာပါသည်။ အွန်လိုင်းဝန်ဆောင်မှုစနစ်များ၊ ဒီဂျစ်တယ်နည်းပညာများကို ကျယ်ပြန့်စွာ အကောင်အထည်ဖော်လာနိုင်သောကြောင့် စီးပွားရေးလုပ်ငန်းများ နှင့်ပြည်သူတို့၏ နေ့စဉ်လူမှုစီးပွားဘဝများတွင် သတင်းအချက်အလက်နှင့် ဆက်သွယ်ရေး နည်းပညာအသုံးပြုမှုအပေါ် များစွာမှီခိုလာကြပါသည်။ ထိုကဲ့သို့ နည်းပညာအသုံးပြုမှုကျယ်ပြန့်လာသည်နှင့်အတူ ဆိုက်ဘာလုံခြုံရေးခြိမ်းခြောက်မှု၊ တိုက်ခိုက်မှုများလည်း များပြားလာခဲ့ပါသည်။

၁၅။ ဉာဏ်ရည်တုနည်းပညာ (AI) ဖွံ့ဖြိုးတိုးတက်လာခြင်းကြောင့် လူသားဖြစ်တည်မှုနှင့် လူနေမှုဘဝပတ်ဝန်းကျင်ကို လွှမ်းမိုးထိခိုက်နိုင်သည့်အခြေအနေများ ကြုံတွေ့လာရပါသည်။ အမျိုးသားလုံခြုံရေးအထိ ထိခိုက်လာနိုင်သောကြောင့် နိုင်ငံအများစုက AI ကိုမူဝါဒ၊ စည်းမျဉ်း၊ စည်းကမ်း၊ ဥပဒေများဖြင့် ထိန်းကျောင်းရန်ကြိုးစားလာကြပါသည်။ သတင်းအချက်အလက်နှင့် နည်းပညာ ဆိုက်ဘာနယ်ပယ်တွင်လည်း စိန်ခေါ်မှုများ များပြားလာသည့်အတွက် မျက်ခြည်မပြတ်စောင့်ကြည့်ရန် လိုအပ်လာပါသည်။ မြန်မာနိုင်ငံအနေဖြင့် AI ၏ သက်ရောက်မှုများစွာ မရှိသေးသော်လည်း ဆိုက်ဘာလုံခြုံရေးကို အထူး သတိပြုလျက်ရှိပါသည်။

၁၆။ သတင်းအချက်အလက်နှင့် ဆက်သွယ်ရေးနည်းပညာ တိုးတက်ထွန်းကားနေသော ယနေ့ခေတ်ကာလတွင် မြန်မာနိုင်ငံအနေဖြင့် ဆက်သွယ်ရေးနည်းပညာဆိုင်ရာ ကဏ္ဍအသီးသီးကို အကျိုးရှိရှိအသုံးချမှုကို ဆက်လက်မြှင့်တင်ပြီး ကြုံတွေ့လာနိုင်သည့် ဆိုက်ဘာခြိမ်းခြောက်မှု၊ တိုက်ခိုက်မှုနှင့်အတူ AI ၏ အသုံးဝင်မှုနှင့် အန္တရာယ်ရှိမှုတို့ကိုပါ လေ့လာသိမြင်၍ ကြိုတင်ပြင်ဆင်ထားရမည်ဖြစ်ပါသည်။[10]

ဆိုက်ဘာလုံခြုံရေး အကောင်အထည်ဖော် ဆောင်ရွက်နေမှုအခြေအနေ

၁၇။ မြန်မာနိုင်ငံတွင် ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ ခြိမ်းခြောက်တိုက်ခိုက်မှုများနှင့် ဆိုက်ဘာရာဇဝတ်မှုခင်းများကို ကြိုတင်ကာကွယ်နိုင်ရန်နှင့် ဖော်ထုတ်အရေးယူနိုင်ရန်၊ လူ့စွမ်းအားအရင်းအမြစ်ဖွံ့ဖြိုးတိုးတက်စေရန်၊ ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ ပတ်ဝန်းကျင်အခြေခံကောင်းများတည်ဆောက်ရန် ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာမူဝါဒတစ်ရပ် ရေးဆွဲထားရှိပြီး ဖြစ်ပါသည်။ ၎င်းမူဝါဒကို နိုင်ငံတော်စီမံအုပ်ချုပ်ရေးကောင်စီ၏ အမိန့်ကြော်ငြာစာအမှတ် ၉၈/၂၀၂၁ ဖြင့် ပြင်ဆင်ဖွဲ့စည်းခဲ့သည့် e-Government အကောင်အထည်ဖော်ရေးလုပ်ငန်းကော်မတီ၏ ကြီးကြပ်မှုဖြင့် ရေးဆွဲခဲ့ပါသည်။[11]

---

[10] ဉာဏ်ရည်တုနည်းပညာဆိုက်ဘာလုံခြုံရေး၊ ပြန်ကြားရေးဝန်ကြီးဌာန၊ 11/03/2023၊ https://www.moi.gov.mm/news/46729 မှကောက်နုတ်ထားပါသည်။ (ကြည့်ရှုရရှိသည့်ရက် ၂၀၂၆ ခုနှစ်၊ ဖေဖော်ဝါရီလ ၁၂ ရက်)

[11] Ibid

၁၈။ နိုင်ငံတော်အစိုးရသည် ဆိုက်ဘာလုံခြုံရေးဥပဒေကို (နိုင်ငံတော်စီမံအုပ်ချုပ်ရေးကောင်စီ ဥပဒေအမှတ် ၁/၂၀၂၁) ဖြင့် ၂၀၂၁ ခုနှစ်၊ ဇန်နဝါရီလ ၁ ရက်နေ့တွင် ပြဋ္ဌာန်းခဲ့ပြီး ၂၀၂၁ ခုနှစ်၊ ဇူလိုင်လ ၃၀ ရက်နေ့မှစတင်၍ အာဏာတည်ခဲ့ပါသည်။ ထိုဥပဒေတွင် ရည်ရွယ်ချက်(၅)ခုရှိပြီး အခန်းပေါင်း (၁၆) ခန်းနှင့် ပုဒ်မပေါင်း ၈၈ ခုပါဝင်သည့်အနက် ဆိုက်ဘာအရင်းအမြစ်၊ အရေးကြီးသတင်းအချက်အလက် အခြေခံအဆောက်အအုံများနှင့် အီလက်ထရောနစ် သတင်းအချက်အလက်များအား လုံခြုံစိတ်ချစွာ အသုံးပြုနိုင်ရန်နှင့် ဆိုက်ဘာအရင်းအမြစ်ကို အခြေခံသော ဒီဂျစ်တယ်စီးပွားရေးစနစ်ကို အထောက်အကူပြုနိုင်စေရေးအတွက် ပြဋ္ဌာန်းချက်များ ပါဝင်သည်ကို တွေ့ရှိရပါသည်။[12]

ဆိုက်ဘာလုံခြုံရေးဥပဒေပါပြဋ္ဌာန်းချက်များ

၁၉။ ဆိုက်ဘာလုံခြုံရေးဥပဒေသည် မျက်မှောက်ကာလ လူမှုဘဝနယ်ပယ်အတွက် အလွန်အရေးကြီးသော ဥပဒေဖြစ်ပါသည်။ မြန်မာနိုင်ငံ၌ သတင်းအချက်အလက် ဆက်သွယ်ရေးကဏ္ဍ ဖွံ့ဖြိုးတိုးတက်လာခဲ့သည်မှာ ဆယ်စုနှစ်နှစ်ခုမက ကာလသို့ရောက်ရှိသည့်အချိန်၌ အများပြည်သူတို့အနေဖြင့် မိမိတို့အသုံးပြုသည့် လူမှုကွန်ရက်များပေါ်၌ သတိပြုရမည့်အချက်များစွာတို့ကို ယင်းဥပဒေတွင် ဖော်ပြထားပါသည်။ ထို့ကြောင့် သတင်းအချက်အလက်နှင့်ဆက်သွယ်ရေးနည်းပညာများကို အသုံးပြုနေသူများအပါအဝင် ပြည်သူများသည် ဆိုက်ဘာလုံခြုံရေးဥပဒေပါ အချက်များအား အထူးအလေးထား မှတ်သားလိုက်နာဆောင်ရွက်ကြရပါမည်။

၂၀။ ဆိုက်ဘာလုံခြုံရေးဥပဒေသည် အွန်လိုင်းအသုံးပြုကြသူများအားလုံး သိရှိလေ့လာလိုက်နာ မှတ်သားကြရမည့်ဥပဒေဖြစ်ပြီး အထူးသဖြင့် သတင်းအချက်အလက် ဆက်သွယ်ရေးနည်းပညာကိုအသုံးပြု၍ နိုင်ငံရေးအမြတ်ထုတ်သူများ၊ ငွေကြေးအကျိုးအမြတ် ရှာဖွေနေကြသူများကို သတိထားရမည့်အချက်များပါဝင်ပါသည်။ ၎င်းဥပဒေသည် အများပြည်သူတစ်ရပ်လုံးနှင့် သက်ဆိုင်ပြီး နိုင်ငံတော်အစိုးရနှင့် နိုင်ငံများက အထူးအလေးထားတိုက်ဖျက်နေသည့် အွန်လိုင်းလိမ်လည်မှုနှင့်လောင်းကစားမှုနှင့်ဆက်စပ်ပါဝင်ပါသည်။ ယခုအခါ နိုင်ငံတော်အစိုးရသည် တရားမဝင်အွန်လိုင်းလိမ်လည်မှုလုပ်ငန်းများအား စုံစမ်းဖော်ထုတ်စစ်ဆေး၍ ထိရောက်စွာ အရေးယူဆောင်ရွက်လျက်ရှိပြီး နယ်စပ်ဒေသများတွင်ဖြစ်ပေါ်လျက်ရှိသည့် အွန်လိုင်းလောင်းကစားမှုနှင့်ငွေကြေးလိမ်လည်မှုများကို အိမ်နီးချင်းနိုင်ငံများနှင့် နိုင်ငံတကာအဖွဲ့အစည်းများက ပူးပေါင်းဆောင်ရွက်လျက်ရှိပါသည်။

[12] Ibid

၂၁။ ဆိုက်ဘာလုံခြုံရေးဥပဒေတွင် အများပြည်သူ သိရှိထားသင့်သည့် အရေးကြီးသောအချက်များမှာ မရှိုးမဖြောင့်သောသဘောဖြင့် ဆိုက်ဘာအရင်းအမြစ်များကို အသုံးပြုပြီး ငွေကြေးတစ်ရပ်ရပ်ကိုခိုးယူခြင်း၊ အကျိုးဖျက်ဆီးခြင်း သို့မဟုတ် အခြားသူတစ်ဦးဦးအား ပြုလုပ်ရန် စေခိုင်းခြင်း၊ ခွင့်ပြုချက်မရှိဘဲ အွန်လိုင်းလောင်းကစားစနစ်တည်ဆောက်ခြင်း၊ ဖွစ်ဘွတ်၊ ယူကျူ၊ တစ်တော့ခ်၊ တယ်လီဂရမ်အစရှိသော လူဦးရေတစ်သိန်းနှင့်အထက်ရှိသည့် ဒီဂျစ်တယ်ပလက်ဖောင်း ဝန်ဆောင်မှုလုပ်ငန်းများ အစရှိသည့် အွန်လိုင်းဝန်ဆောင်မှုလုပ်ငန်းများ လုပ်ကိုင်ပါက တရားဝင်မှတ်ပုံတင် လိုင်စင်လျှောက်ထားခြင်း၊ လျှောက်ထားရန်ပျက်ကွက်ကြောင်း တွေ့ရှိပါက အရေးယူခြင်းစသည့် ပြစ်မှုပြစ်ဒဏ်၊ ထောင်ဒဏ်များပါဝင်ပါသည်။

၂၂။ ၎င်းဥပဒေတွင် ဒီဂျစ်တယ်ပလက်ဖောင်းဝန်ဆောင်မှုလုပ်ငန်းဆောင်ရွက်သူသည် ဝန်ဆောင်မှုပလက်ဖောင်းများတွင် အမုန်းတရားကိုဖြစ်စေသော၊ စည်းလုံးညီညွတ်မှုကို ပျက်ပြားစေသော သို့မဟုတ် တည်ငြိမ်အေးချမ်းမှုကို ပျက်ပြားစေသော သတင်းအချက်အလက်များဖြစ်ပေါ်ခြင်း၊ မမှန်သတင်း သို့မဟုတ် ကောလာဟလသတင်းများဖြစ်ပေါ်ခြင်း၊ အများပြည်သူ ကြည့်ရှုရန် မသင့်လျော်သော သတင်းအချက်အလက်များကို ဖော်ပြခြင်း၊ လိင်ပိုင်းဆိုင်ရာ ရည်ရွယ်ချက်ဖြင့် ဖော်ပြသော ကလေးသူငယ်များ၏ ညစ်ညမ်းပုံ၊ ညစ်ညမ်းဗီဒီယို၊ စာသားများ သို့မဟုတ် သင်္ကေတများကို တစ်နည်းနည်းဖြင့်ဖော်ပြခြင်း၊ တည်ဆဲဥပဒေတစ်ရပ်ရပ်နှင့် ဆန့်ကျင်သည့် သတင်းအချက်အလက်များကို ဖော်ပြခြင်း သို့မဟုတ် ဥပဒေနှင့် မညီသော ပြုလုပ်မှုကို ပြုလုပ်ခြင်း၊ လူပုဂ္ဂိုလ်တစ်ဦးတစ်ယောက်၏ လူမှုရေး သို့မဟုတ် စီးပွားရေးကို ထိခိုက်နစ်နာစေရန် ရည်ရွယ်ဖော်ပြသော သတင်းအချက်အလက်နှင့်စပ်လျဉ်းသည့်၊ မူပိုင်ခွင့်ဆိုင်ရာ အခွင့်အရေးချိုးဖောက်ခြင်းနှင့်ပတ်သက်သည့် တိုင်ကြားချက်များဖြစ်ပေါ်ခြင်း၊ အကြမ်းဖက်မှုဖြစ်ပေါ်စေရန် လှုံ့ဆော်ခြင်း၊ ကျူးလွန်ခြင်း၊ အားထုတ်ခြင်း၊ အားပေးကူညီခြင်း သို့မဟုတ် ကြံရာပါအဖြစ် ဆောင်ရွက်ခြင်းတို့နှင့်ပတ်သက်သည့် မှတ်သားလိုက်နာရမည့် အချက်များပါဝင်သည်ကို တွေ့ရှိရပါသည်။

၂၃။ ထို့အပြင် ဆိုက်ဘာလုံခြုံရေးကို ခြိမ်းခြောက်ခြင်း၊ တိုက်ခိုက်ခြင်း သို့မဟုတ် ဆိုက်ဘာလုံခြုံရေးကို အလွဲသုံးစားပြုလုပ်ခြင်းစသည်တို့နှင့်ပတ်သက်သည့် အရေးကြီးသော အချက်အလက်များ၊ တာဝန်ရှိအဖွဲ့အစည်းများ၊ ဆောင်ရွက်ရမည့်အချက်များ၊ စီမံခန့်ခွဲရေးနည်းလမ်းဖြင့် အရေးယူမှုများ၊ အယူခံဝင်မှုနှင့် ပြစ်မှုပြစ်ဒဏ်များစသည်တို့ ကျယ်ပြန့်စွာပါဝင်ပါသည်။ ထို့ကြောင့် သတင်းအချက်အလက်နှင့် နည်းပညာထွန်းကားနေသော ယနေ့ကာလ၌ အဆိုပါ

နည်းပညာများအား အသုံးပြုနေကြသူများအားလုံးအနေဖြင့် ဆိုက်ဘာလုံခြုံရေးဥပဒေပါအချက်များကို လေ့လာမှတ်သား အလေးထား လိုက်နာဆောင်ရွက်ကြရပါမည်။[13]

ကမ္ဘာတွင် မြန်မာနိုင်ငံ၏ဆိုက်ဘာလုံခြုံရေးအဆင့်

၂၄။ ကုလသမဂ္ဂအောက်ရှိ အဖွဲ့အစည်းတစ်ခုဖြစ်သော နိုင်ငံတကာသတင်းနှင့် ဆက်သွယ်ရေးသမဂ္ဂ (International Telecommunication Union – ITU) က အဖွဲ့ဝင်နိုင်ငံပေါင်း ၁၉၄ နိုင်ငံ၏ ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ ပြင်ဆင်ဆောင်ရွက်ထားရှိမှုများကို အကဲဖြတ်အမှတ်ပေးကာ ''၂၀၂၄ ခုနှစ် ဆိုက်ဘာလုံခြုံရေးညွှန်းကိန်း''ကို ထုတ်ပြန်ခဲ့ပါသည်။ နိုင်ငံများ၏ ဆိုက်ဘာလုံခြုံရေးညွှန်းကိန်းကို တိုင်းတာရာတွင် မဏ္ဍိုင်ကြီး (၅)ရပ်အပေါ် အခြေခံတိုင်းတာပါသည်။ ယင်းမဏ္ဍိုင်ကြီး (၅)ရပ်မှာ-

(က) **ဥပဒေဆိုင်ရာ (Legal)**။ ဥပဒေဆိုင်ရာတိုင်းတာမှုတွင် ဆိုက်ဘာရာဇဝတ်မှုဆိုင်ရာ ဥပဒေများ၊ ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာစည်းမျဉ်းစည်းကမ်းများနှင့် ဆိုက်ဘာလုံခြုံရေးလေ့ကျင့်သင်ကြားမှုများနှင့်သက်ဆိုင်သည့် ဥပဒေများရေးဆွဲထားခြင်းရှိ/မရှိ၊ ခိုင်မာအားကောင်းမှုရှိ/မရှိတို့ကိုအကဲဖြတ်ပါသည်။

(ခ) **နည်းပညာဆိုင်ရာ (Technical)**။ နည်းပညာပိုင်းဆိုင်ရာ အကဲဖြတ်ရာတွင် ကွန်ပျူတာထိခိုက်မှု တုံ့ပြန်မှုအဖွဲ့ (Computer Incident Response Team– CIRT)၊ ကွန်ပျူတာ လုံခြုံရေးဆိုင်ရာ ထိခိုက်မှုတုံ့ပြန်မှုအဖွဲ့ (Computer Security Incident Response Team– CSIRT)နှင့် ကွန်ပျူတာ အရေးပေါ် တုံ့ပြန်မှုအဖွဲ့ (Computer Emergency Response Team– CERT)များကို နိုင်ငံတော်အဆင့်၊ ဒေသန္တရအဆင့်၊ ဌာနအဖွဲ့အစည်းအဆင့်စသည်ဖြင့် ဖွဲ့စည်းဆောင်ရွက်နေမှုအခြေ အနေများ၊ ဆိုက်ဘာအဖွဲ့အစည်းများဖွဲ့စည်းရန် စံသတ်မှတ်ချက်များ၊ ဆိုက်ဘာ ကျွမ်းကျင်ပညာရှင်ဆိုင်ရာ စံနှုန်းသတ်မှတ်ချက်များစသည်တို့ဖြင့် တိုင်းတာ အကဲဖြတ်ပါသည်။

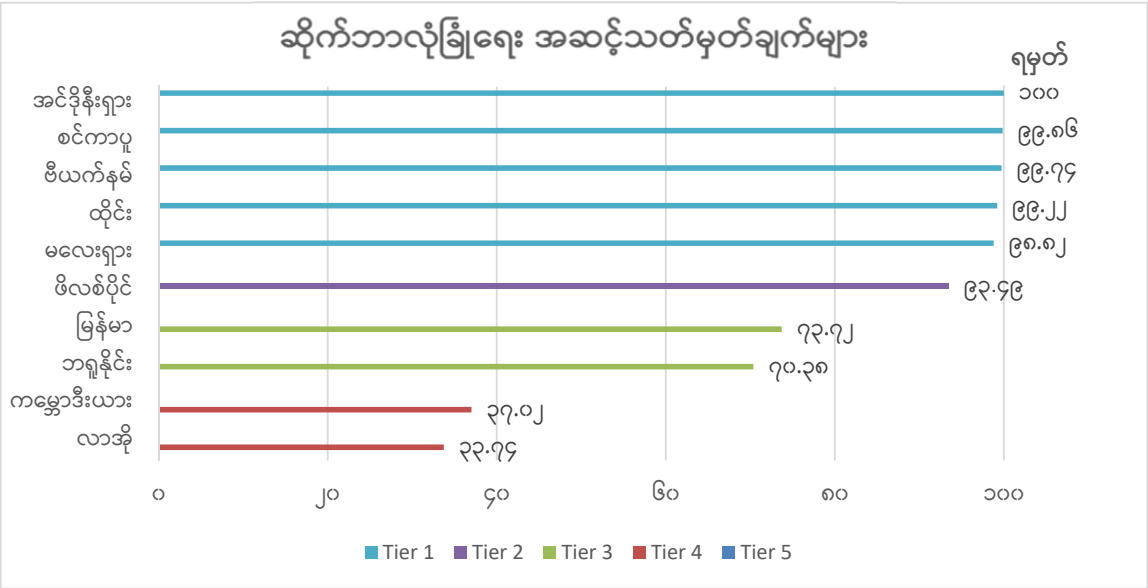
(ဂ) **အဖွဲ့အစည်းဆိုင်ရာ (Organizational)**။ အဖွဲ့အစည်းဆိုင်ရာတိုင်းတာရာတွင် ဖွဲ့စည်းထားရှိသည့် အဖွဲ့များ၏ မဟာဗျူဟာချမှတ် ဆောင်ရွက်နေမှု၊ ဆိုက်ဘာလုပ်ငန်းအတွက် တာဝန်ရှိသည့် အဖွဲ့အစည်းများ ဖွဲ့စည်းထားရှိမှုနှင့် ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာရှုထောင့်များဖြင့် တိုင်းတာအမှတ်ပေးပါသည်။

[13] ဆိုက်ဘာအရင်းအမြစ်အီလက်ထရောနစ်ဥပဒေနှင့်အညီ လုံခြုံစိတ်ချလိုက်နာအသုံးပြု၊ ပြန်ကြားရေးဝန်ကြီးဌာန၊ 08/05/2025၊ https://www.moi.gov.mm/news/73231 မှကောက်နုတ်ထားပါသည်။ (ကြည့်ရှုရရှိသည့်ရက် ၂၀၂၆ ခုနှစ်၊ ဇန်နဝါရီလ ၁၀ ရက်)

(ဃ) **စွမ်းဆောင်ရည်မြှင့်တင်မှုဆိုင်ရာ (Capacity Development)**။ စွမ်းဆောင်ရည်မြှင့်တင်မှုဆိုင်ရာကဏ္ဍတွင် သုတေသနနှင့် ဖွံ့ဖြိုးရေး (R&D) ဆောင်ရွက်နေမှုအခြေအနေများ၊ အများပြည်သူသို့ပညာပေးဆောင်ရွက်မှု၊ ဆိုက်ဘာကျွမ်းကျင်ပညာရှင်များ လေ့ကျင့်ပျိုးထောင်နေမှု၊ အမျိုးသားပညာရေးတွင် ထည့်သွင်းပါဝင်မှုနှင့်ကျောင်းသင်ရိုးညွှန်းတမ်းများတွင် ထည့်သွင်းသင်ကြားပေးမှုအခြေအနေများ၊ မက်လုံးပေး၊ အားပေးဆောင်ရွက်နေမှုအခြေအနေများနှင့် အခြားနိုင်ငံများမှ ကူးယူခြင်းမပြုဘဲ မိမိနိုင်ငံမှာပင် တီထွင်ဖော်ထုတ်နိုင်မှုအခြေအနေများ စသည်တို့အပေါ်မူတည်ကာ တိုင်းတာအမှတ်ပေးပါသည်။

(င) **ပူးပေါင်းဆောင်ရွက်မှုဆိုင်ရာ (Cooperation)**။ ပူးပေါင်းဆောင်ရွက်မှုဆိုင်ရာကဏ္ဍအား အမှတ်ပေးရာတွင် နိုင်ငံများအကြားတွင် သဘောတူစာချုပ်များ ချုပ်ဆိုဆောင်ရွက်နေမှုအခြေအနေများ၊ နိုင်ငံတကာတွင် ပူးပေါင်းပါဝင်နေသည့် အခြေအနေများ၊ အစိုးရအနေဖြင့် ဆိုက်ဘာလုပ်ငန်းများတွင် ပုဂ္ဂလိကကဏ္ဍနှင့် ပူးပေါင်းဆောင်ရွက်နေသည့် အခြေအနေများ၊ နိုင်ငံရှိ ဆိုက်ဘာအဖွဲ့အစည်းများအကြား ပူးပေါင်းဆောင်ရွက်မှုအခြေအနေများ စသည်တို့ဖြင့် အကဲဖြတ် တိုင်းတာအမှတ်ပေးပါသည်။

၂၅။ ၂၀၂၄ ခုနှစ်တွင် ITU မှထုတ်ပြန်ထားသည့် ဆိုက်ဘာလုံခြုံရေးအညွှန်းကိန်းအရ အာဆီယံနိုင်ငံများ၏ ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ အဆင့်သတ်မှတ်ချက်များအား အောက်ပါ Bar Chart ဖြင့် ဖော်ပြအပ်ပါသည်-



၂၆။ ITU ၏ Report အရ အထက်တွင်ဖော်ပြခဲ့သောအချက် (၅)ချက်ကို အခြေခံ၍ နိုင်ငံများကိုရမှတ် ၀ မှ ၁၀၀ အထိပေးထားပြီး ရမှတ်အလိုက် Tier အဆင့်သတ်မှတ်ချက် အုပ်စု(၅)ခုဖြင့် အောက်ပါအတိုင်းခွဲခြားသတ်မှတ်ထားပါသည်-

(က) **Tier 1:** စံပြအဆင့် (Role-modelling)တွင် ရမှတ် ၉၅ မှ ၁၀၀ ကြားဖြစ်ပြီး အင်ဒိုနီးရှား၊ စင်ကာပူ၊ ဗီယက်နမ်၊ ထိုင်းနှင့် မလေးရှားနိုင်ငံတို့ ပါဝင်ပါသည်။ ဆိုက်ဘာလုံခြုံရေး၏ မဏ္ဍိုင်ကြီး ၅ ရပ်စလုံးတွင် အမှတ်ပြည့်နီးပါးဖြင့် စံပြဖြစ်နေသောအုပ်စု ဖြစ်သည့်အပြင် ခိုင်မာသောဥပဒေများ၊ ခေတ်မီနည်းပညာနှင့် အဖွဲ့အစည်းဆိုင်ရာ စနစ်တကျပြင်ဆင်ထားမှုများကြောင့် ကမ္ဘာ့အဆင့်တွင်ပင် ထိပ်တန်းမှ ရပ်တည်နေသည့်နိုင်ငံများဖြစ်ကြပါသည်။

(ခ) **Tier 2:** တိုးတက်မြင့်မားသောအဆင့်(Advancing) တွင် ဖိလစ်ပိုင်နိုင်ငံသည် ရမှတ် ၈၅ မှ ၉၅ အတွင်းရရှိကာ ဆိုက်ဘာလုံခြုံရေးလုပ်ငန်းစဉ်များကို အရှိန်အဟုန်ဖြင့် တိုးမြှင့်လုပ်ဆောင်နေပြီး အားကောင်းသော အခြေခံအဆောက်အအုံများရှိနေပြီဖြစ်သော်လည်း Tier 1 အဆင့်သို့ရောက်ရှိရန် ပူးပေါင်းဆောင်ရွက်မှုနှင့်စွမ်းဆောင်ရည်မြှင့်တင်မှုကဏ္ဍအချို့တွင် အနည်းငယ်မျှသာ ဆက်လက်ဖြည့်ဆည်းရန် လိုအပ်နေသောအုပ်စုဖြစ်ပါသည်။

(ဂ) **Tier 3:** အခြေခံတည်ဆောက်နေဆဲအဆင့်(Establishing)တွင် မြန်မာနိုင်ငံနှင့် ဘရူနိုင်းနိုင်ငံတို့ပါဝင်ပြီး ရမှတ် ၅၅ မှ ၈၅ အတွင်းရရှိထားကာ ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာမူဘောင်များကို အခြေခံကျကျ စတင်အခြေချနိုင်ပြီဖြစ်သော်လည်းနည်းပညာ၊အဖွဲ့အစည်းဆိုင်ရာနှင့် စွမ်းဆောင်ရည်မြှင့်တင်မှုကဏ္ဍများတွင် တိုးတက်ရန် အလားအလာများစွာ (Potential Growth) လိုအပ်နေသေးသည့်အပြင် နိုင်ငံတော်အဆင့် ဆိုက်ဘာလုံခြုံရေးကို ခိုင်မာအောင် တည်ဆောက်ဆဲအဆင့် ဖြစ်ပါသည်။

(ဃ) **Tier 4:** ဖွံ့ဖြိုးမှုအဆင့် (Evolving) တွင် ကမ္ဘောဒီးယားနှင့် လာအိုနိုင်ငံတို့သည် ရမှတ် ၂၀ မှ ၅၅ အတွင်းရှိကာ ၎င်းတို့သည် ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ ကတိကဝတ်များကို စတင်အကောင်အထည်ဖော်နေသော ဖွံ့ဖြိုးမှုအဆင့်တွင် ရှိနေသည့်အပြင် ဥပဒေကြောင်းအရ စတင်မှုအချို့ရှိသော်လည်း နည်းပညာ၊ စွမ်းဆောင်ရည်မြှင့်တင်မှုနှင့် အဖွဲ့အစည်းဆိုင်ရာမူဝါဒများကို ပိုမိုမြှင့်တင်ရန် လိုအပ်နေသည့်အုပ်စုဖြစ်ပါသည်။

(c) **Tier 5:** တည်ဆောက်ဆဲအဆင့်(Building) သည် ရမှတ် ၂၀ အောက် ရရှိသော နိုင်ငံများဖြစ်ပြီး ဆိုက်ဘာလုံခြုံရေးအခြေခံအဆောက်အအုံများကို စတင်ပျိုးထောင်နေရသည့်အဆင့်ဖြစ်ပြီး အာဆီယံ ၁၀ နိုင်ငံလုံးသည် အနည်းဆုံး Tier 4 အဆင့်သို့ ရောက်ရှိပြီးဖြစ်သောကြောင့် ဤ Tier 5 အဆင့်တွင် ပါဝင်ခြင်းမရှိပါ။[14]

နိဂုံး

၂၇။ ဆိုက်ဘာလုံခြုံရေးသည် နည်းပညာပိုင်းဆိုင်ရာ အကာအကွယ်ပေးမှုအပြင် နိုင်ငံတော်၏ ပုံရိပ်၊ လူမှုစီးပွားဘဝတည်ငြိမ်မှုနှင့် အမျိုးသားလုံခြုံရေးတို့အတွက် အခြေခံအုတ်မြစ်တစ်ခု ဖြစ်ပါသည်။ နည်းပညာနှင့် AI ကဏ္ဍများ အရှိန်အဟုန်ဖြင့် တိုးတက်နေသည်နှင့်အမျှ ဆိုက်ဘာခြိမ်းခြောက်မှုများသည်လည်း ပိုမိုနက်နဲ ရှုပ်ထွေးလာပါသည်။ ထို့ကြောင့် အစိုးရ၊ ပုဂ္ဂလိကနှင့် ပြည်သူများအနေဖြင့် ၂၀၂၅ ခုနှစ်၊ ဆိုက်ဘာလုံခြုံရေးဥပဒေပါ ပြဋ္ဌာန်းချက်များကို တိကျစွာလိုက်နာခြင်းဖြင့် နိုင်ငံသားတို့၏ ဒီဂျစ်တယ်အခွင့်အရေးနှင့် အချက်အလက်လုံခြုံမှုကို ပူးပေါင်းကာကွယ်ကြရမည် ဖြစ်ပါသည်။ အဓိကအားဖြင့် ဥပဒေနှင့်အညီ ကျင့်ကြံနေထိုင်ခြင်းသည် ဆိုက်ဘာရာဇဝတ်မှုများတွင် ပါဝင်ပတ်သက်မိခြင်း သို့မဟုတ် သားကောင်ဖြစ်ခြင်းတို့မှ ကင်းဝေးစေမည့် အကောင်းဆုံးအကာအကွယ်ပင် ဖြစ်ပါသည်။ ဆိုက်ဘာလုံခြုံရေးသည် နည်းပညာဆိုင်ရာ ပြဿနာတစ်ခုမျှသာ မဟုတ်ဘဲ၊ ယနေ့ခေတ် လူသားတိုင်း၏ တာဝန်ဖြစ်နေပါသည်။ ဆိုက်ဘာလုံခြုံရေး အသိပညာမြင့်မားလာခြင်းသည် ဘေးကင်းလုံခြုံသော ဒီဂျစ်တယ် လူ့အဖွဲ့အစည်းနှင့် ခိုင်မာသော ဒီဂျစ်တယ်စီးပွားရေးစနစ်ကို တည်ဆောက်ရာတွင် အဓိကကျသော တွန်းအားတစ်ခုဖြစ်လာမည် ဖြစ်ပါကြောင်း ရေးသားတင်ပြအပ်ပါသည်။

စီးပွားရေးဌာနစု
သုတေသနဌာန
ပြည်သူ့လွှတ်တော်ရုံး

[14] ITU, Global Cybersecurity Index 2024 , https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf မှကောက်နုတ်ထားပါသည်။ (ကြည့်ရှုရရှိသည့်ရက် ၂၀၂၆ ခုနှစ်၊ မေလ ၁ ရက်)

သတိပြုရန်

ဤသတင်းအချက်အလက်သည် လွတ်တော်ဆိုင်ရာတာဝန်များကို ဆောင်ရွက်ရာတွင် အထောက်အကူပြုရန်အတွက်ဖြစ်ပါသည်။ ပုဂ္ဂိုလ်ရေးဆိုင်ရာကိစ္စတစ်စုံတစ်ခုအတွက် အသုံးပြုရန် မဟုတ်ပါ။ အချိန်နှင့်တပြေးညီ နောက်ဆုံးရသတင်းဖြစ်မည်ဟု သတ်မှတ်မထားသင့်ပါ။ ဤအချက်အလက်များအား တရားဝင်သို့မဟုတ် ပညာရှင်ဆိုင်ရာ အကြံပေးချက်အဖြစ် မသတ်မှတ်သင့်ပါ။ လွတ်တော် သုတေသနဝန်ဆောင်မှုသည် စာတမ်းတိုများတွင်ပါဝင်သော အကြောင်းအရာများနှင့်စပ်လျဉ်း၍ လွတ်တော်ဝန်ထမ်းများနှင့်ဆွေးနွေးမှုများ ပြုလုပ်ပေးနိုင်ပါသည်။ အများပြည်သူနှင့် ဆွေးနွေးမှုများ ပြုလုပ်ခြင်းမရှိပါ။