ငွေကြေးဆိုင်ရာစုံစမ်းထောက်လှမ်းရေးအဖွဲ့
Financial Intelligence Unit - FIU

မဟာဗျူဟာခွဲခြမ်းစိတ်ဖြာမှုအစီရင်ခံစာ

အွန်လိုင်းလိမ်လည်မှုများနှင့်ဆက်နွယ်သည့် ငွေကြေးခဝါချမှုလားရာများ

၂၀၂၄ ခုနှစ်၊ ဧပြီလ

SR/001/2024

www.mfiu.gov.mm

မာတိကာ

၁ နိဒါန်း...၁
၂ ရည်ရွယ်ချက် ၁
၃ သတင်းအချက်အလက်အသုံးပြုမှု ၂
၄ အွန်လိုင်းလိမ်လည်မှုဖြစ်ပွားမှုအခြေအနေ ၂
၅ အွန်လိုင်းလိမ်လည်မှုနှင့်ဆက်နွယ်သည့် သံသယဖြစ်ဖွယ်လွှဲပြောင်းဆောင်ရွက်မှု သတင်းပို့ချက်(STR) လက်ခံရရှိမှု...၂
၆ နေရာဒေသအလိုက် အွန်လိုင်းလိမ်လည်မှုနှင့်ဆက်နွယ်သည့် သံသယဖြစ်ဖွယ်လွှဲပြောင်း ဆောင်ရွက်မှု သတင်းပို့ချက်(STR) လက်ခံရရှိမှု ၃
၇ အွန်လိုင်းလိမ်လည်မှုများနှင့်စပ်လျဉ်းသည့် Operational Analysis Report ဖြန့်ဝေနိုင်မှု ၄
၈ ဌာနများအလိုက် အွန်လိုင်းလိမ်လည်မှုများနှင့်စပ်လျဉ်းသည့် Operational Analysis Report (OAR) ဖြန့်ဝေနိုင်မှု ၄
၉ ဖော်ထုတ်တွေ့ရှိရသည့် အွန်လိုင်းလိမ်လည်မှုနည်းလမ်းများ (CEF Typologies) ၅
၉.၁ နည်းလမ်း(၁)။ Application များ၊ Website အတုများအသုံးပြု၍ သတင်းအချက်အလက်များ ရယူပြီး ငွေကြေးများလိမ်လည်ခြင်း ၅
၉.၂ နည်းလမ်း(၂)။ ဘဏ်နှင့် ငွေရေးကြေးရေးအဖွဲ့အစည်းများ သို့မဟုတ် မိုဘိုင်းငွေကြေး ဝန်ဆောင်မှု လုပ်ငန်း များ၏ ဝန်ထမ်းအယောင်ဆောင်၍ လူမှုကွန်ရက်နှင့် တယ်လီဖုန်း ဆက်သွယ်မှုများမှ တစ်ဆင့်လိမ်လည်ခြင်း ၈
၉.၃ နည်းလမ်း(၃)။ အွန်လိုင်းပေါ်တွင် ခင်မင်ရင်းနှီးအောင်ပြုလုပ်၍ လိမ်လည်ခြင်း ၉
၉.၄ နည်းလမ်း(၄)။ အရောင်းအဝယ်လုပ်ငန်းများ၊ ရင်းနှီးမြှုပ်နှံမှုလုပ်ငန်းများကို အကြောင်းပြု၍ လိမ်လည်ခြင်း...၁၀
၉.၅ နည်းလမ်း (၅)။ အလုပ်အကိုင်အခွင့်အလမ်းများရရှိမည်ဟု အကြောင်းပြု၍ လိမ်လည်ခြင်း ၁၁
၉.၆ အခြားနည်းလမ်းများ...၁၁
၁၀ အွန်လိုင်းလိမ်လည်မှုနှင့် ငွေကြေးခဝါချမှုအကြားဆက်နွယ်မှု ၁၂
၁၁ အခြားမှုခင်းများနှင့်ဆက်နွယ်မှု ၁၂
၁၂ အွန်လိုင်းလိမ်လည်ရာတွင် အသုံးပြုသည့် ငွေကြေးခဝါချမှုနည်းလမ်းများနှင့် လားရာများ.................၁၃
၁၃ သုံးသပ်တင်ပြချက် ၁၄
၁၄ နိဂုံး...၁၄
နောက်ဆက်တွဲ(က) ၁၅
နောက်ဆက်တွဲ(ခ) ၁၆
နောက်ဆက်တွဲ(ဂ) ၂၀

အွန်လိုင်းလိမ်လည်မှုများနှင့်ဆက်နွယ်သည့်ငွေကြေးခဝါချမှုလားရာများ

၁ နိဒါန်း

၁။ ကမ္ဘာပေါ်တွင် ကိုဗစ်-၁၉ ကူးစက်ရောဂါကူးစက်ပြန့်ပွားချိန်၌မှစ၍ လှုပ်ရှားသွားလာမှုများကို ကန့်သတ် ထိန်းချုပ်ခြင်းများကြောင့် လူသားများ၏ အင်တာနက်အွန်လိုင်းအသုံးပြုမှုနှင့် လူမှုကွန်ရက် Social Media သုံးစွဲမှုများမှာ တစ်ဟုန်ထိုး မြင့်တက်လာခဲ့ပါသည်။ Social Media များ၏ ကျယ်ကျယ်ပြန့်ပြန့်ဆက်သွယ်နိုင်မှုနှင့် အင်တာနက်ဆက်သွယ်ရေးကိုအခြေခံသည့် Mobile Banking ကဲ့သို့သော ငွေကြေးဝန်ဆောင်မှုလုပ်ငန်းများ၏ လွယ်ကူလျင်မြန်စွာ ငွေလွှဲပြောင်းနိုင်မှုများသည် Online Trading လုပ်ငန်းများကို ဖွံ့ဖြိုးတိုးတက်လာစေမှုနှင့်အတူ လိမ်လည်မှုကို ကျူးလွန်သည့် ဒုစရိုက်သမားများအတွက်လည်း အသုံးချနိုင်မည့် အခွင့်အလမ်းများဖြစ်လာစေပါသည်။

၂။ အင်တာနက်အွန်လိုင်းဆက်သွယ်ရေးအပေါ် အသုံးချ၍ ကျူးလွန်သည့် လိမ်လည်မှုမှုခင်းများမှာ နှစ်စဉ်တိုးတက်များပြားလာရာ ယင်းမှုခင်းများနှင့်ဆက်နွယ်သည့် သံသယဖြစ်ဖွယ်လွှဲပြောင်းဆောင်ရွက်မှု သတင်းပို့ချက်များလည်း တိုးတက်များပြားလာပါသည်။ လိမ်လည်မှုသည် ၂၀၁၄ ခုနှစ် ငွေကြေးခဝါချမှုတိုက်ဖျက်ရေးဥပဒေအရ ငွေကြေးခဝါချမှုနှင့်သက်ဆိုင်သည့် ပြစ်မှုဖြစ်ပါသည်။ အွန်လိုင်းလိမ်လည်မှု မှုခင်းများ တိုးတက်များပြားလာခြင်းကြောင့် ယင်းမှုခင်းများမှ ထွက်ရှိသည့် ငွေမဲများ၏စီးဆင်းမှု (Illicit Financial Flow) သည် ငွေကြေးခဝါချမှုအတွက် ခြိမ်းခြောက်မှု တစ်ရပ်ဖြစ်လာပါသည်။ ဤအစီရင်ခံစာတွင် အွန်လိုင်းဆက်သွယ်ရေးအပေါ် အသုံးချသည့် လိမ်လည်မှုများနှင့် ဆက်နွယ်သည့် ငွေကြေးခဝါချမှု အလားအလာများကို ဖော်ထုတ်ထားပါသည်။

၂ ရည်ရွယ်ချက်

၃။ ဤအစီရင်ခံစာ၏ ရည်ရွယ်ချက်မှာ အွန်လိုင်းလိမ်လည်မှုနှင့်ဆက်နွယ်သည့် ငွေကြေးခဝါချမှု၏ လားရာများကို နားလည်သိရှိပြီး အောက်ပါအတိုင်း အထောက်အကူဖြစ်စေရန် ရည်ရွယ်ပါသည် -

(က) ကြီးကြပ်ရေးအာဏာပိုင်များ၏ AML/CFT ဆိုင်ရာ ကြီးကြပ်ရေးလုပ်ငန်းများနှင့် သက်ဆိုင်ရာကဏ္ဍအလိုက် ဆုံးရှုံးနိုင်ခြေအန္တရာယ်အကဲဖြတ်ရေး လုပ်ငန်းများ အကောင်အထည်ဖော်ဆောင်ရွက်ရာတွင် အထောက်အကူဖြစ်စေရန်၊

(ခ) သတင်းပို့အဖွဲ့အစည်းများ၏ CDD လုပ်ငန်းစဉ်များနှင့် သတင်းပို့ခြင်းလုပ်ငန်းများ ဆောင်ရွက်ရာတွင် အထောက်အကူဖြစ်စေရန်၊

(ဂ) တရားဥပဒေစိုးမိုးရေးအဖွဲ့အစည်းများ၏ ငွေကြေးဆိုင်ရာစုံစမ်းစစ်ဆေးခြင်း (Financial Investigation) ဆောင်ရွက်ရာတွင် အထောက်အကူဖြစ်စေရန်။

၃ သတင်းအချက်အလက်အသုံးပြုမှု

၄။ ၂၀၂၃ ခုနှစ်အတွင်း ငွေကြေးဆိုင်ရာစုံစမ်းထောက်လှမ်းရေးအဖွဲ့(FIU)က လက်ခံရရှိသည့် သံသယဖြစ်ဖွယ်လွှဲပြောင်းဆောင်ရွက်မှုသတင်းပို့ချက် (STR)များ၊ အွန်လိုင်းလိမ်လည်မှုနှင့် ဆက်နွယ်သည့်လုပ်ငန်းနယ်ပယ်စိစစ်ချက်အစီရင်ခံစာ (Operational Analysis Reports) များ၊ ပြန်ကြားရေးဝန်ကြီးဌာနက အများပြည်သူသို့ ထုတ်ပြန်သည့် သတင်းအချက်အလက်[1]များနှင့် Open Source မှ ရရှိသည့် သတင်းအချက်အလက်များကို အခြေခံထားပါသည်။

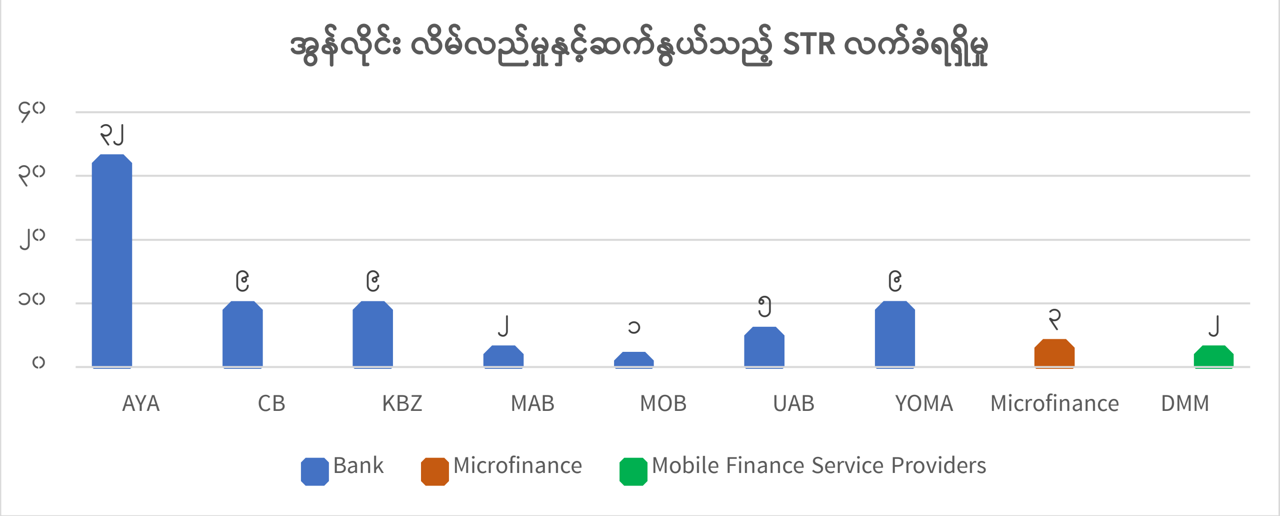
၄ အွန်လိုင်းလိမ်လည်မှုဖြစ်ပွားမှုအခြေအနေ

၅။ အွန်လိုင်းလိမ်လည်မှုများနှင့်ပတ်သက်၍ မူခင်းရဲတပ်ဖွဲ့ထံ နယ်မြေရဲစခန်းများမှ ထင်မြင်ချက် တောင်းခံသည့် သတင်းအချက်အလက်များအရ ၂၀၁၉ ခုနှစ်တွင် (၁၁၆)မှု၊ ၂၀၂၀ ပြည့်နှစ်တွင် (၁၄၂)မှု၊ ၂၀၂၁ ခုနှစ်တွင် (၇၈)မှု၊ ၂၀၂၂ ခုနှစ်တွင် (၁၂၉)မှုနှင့် ၂၀၂၃ ခုနှစ်၊ ဒီဇင်ဘာလအထိ (၁၇၈)မှု၊ စုစုပေါင်း (၆၄၃)မှုခန့် ဖြစ်ပွားခဲ့ကြောင်း သိရှိရပါသည်။ အွန်လိုင်းလိမ်လည်မှုများမှာ ပြည်သူလူထု အကြားတွင် အထက်ပါ စာရင်းဇယားများနှင့် နှစ်ဆကျော်ခန့် ဖြစ်ပွားနေမည်ဟု ခန့်မှန်းရပါသည်။ လိမ်လည်ခံရသည့် ငွေပမာဏနည်းပါးခြင်း၊ ရဲစခန်းများနှင့် တရားရုံးများအတွက် အချိန်မပေး နိုင်ခြင်း၊ ဥပဒေအရနစ်နာသူမှ တရားလိုပြုလုပ်ဆောင်ရွက်ရန် လိုအပ်ခြင်းတို့ကြောင့် အမှုဖွင့် တိုင်ကြားခြင်းမရှိသည့်မှုခင်း များစွာရှိနေနိုင်ပါသည်။ အွန်လိုင်းလိမ်လည်မှုများကြောင့် ငွေကြေး ဆုံးရှုံးနစ်နာမှုများမှာ နှစ်စဉ် မြန်မာကျပ်ငွေ ၅ ဘီလီယံနှင့်အထက်တွင် ရှိနေနိုင်ကြောင်း ခန့်မှန်း ရပါသည်။

၅ အွန်လိုင်းလိမ်လည်မှုနှင့်ဆက်နွယ်သည့် သံသယဖြစ်ဖွယ်လွှဲပြောင်းဆောင်ရွက်မှု သတင်းပို့ချက်(STR) လက်ခံရရှိမှု

၆။ ငွေကြေးဆိုင်ရာ စုံစမ်းထောက်လှမ်းရေးအဖွဲ့(FIU)အနေဖြင့် ၂၀၂၃ ခုနှစ်အတွင်း ငွေသား လွှဲပြောင်းဆောင်ရွက်မှုနှင့်ပတ်သက်သည့် သံသယဖြစ်ဖွယ် လွှဲပြောင်းဆောင်ရွက်မှု သတင်းပို့ချက် (STR)(၁၀၉၂)စောင် လက်ခံရရှိခဲ့ပါသည်။ ယင်း STR များအနက်မှ အွန်လိုင်းလိမ်လည်မှုများနှင့် ဆက်နွယ်သည့် STR(၇၂)စောင်လက်ခံရရှိခဲ့ပါသည်။ သတင်းပို့အဖွဲ့အစည်းများအလိုက် အွန်လိုင်း လိမ်လည်မှုနှင့်ဆက်နွယ်သည့် STR လက်ခံရရှိမှုအား အောက်ဖော်ပြပါပုံ(၁)တွင် ဖော်ပြထားရှိပါသည်။ အွန်လိုင်း လိမ်လည်မှုနှင့်ဆက်နွယ်သည့် STR များနှင့်စပ်လျဉ်း၍ လွှဲပြောင်းမှုတန်ဖိုးပမာဏ စိစစ်မှုများအား နောက်ဆက်တွဲ(က) ဖြင့် ဖော်ပြထားပါသည်။

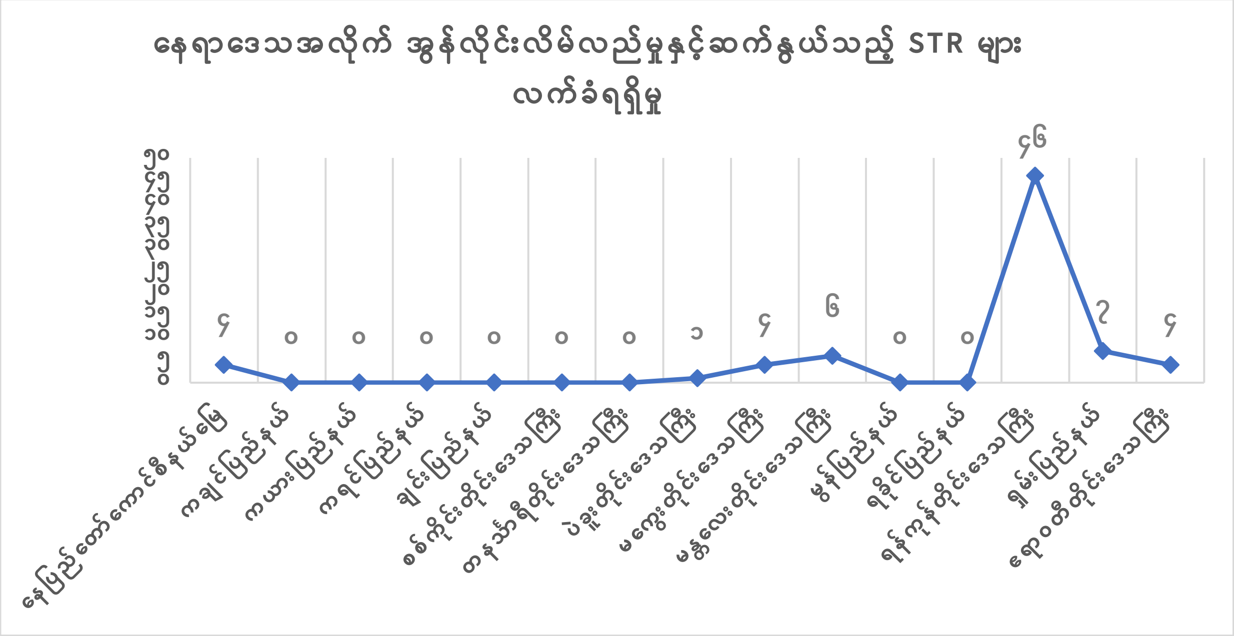
[1] https://www.moi.gov.mm/news/46515



ပုံ(၁)သတင်းပို့အဖွဲ့အစည်းများအလိုက် အွန်လိုင်း လိမ်လည်မှုနှင့်ဆက်နွယ်သည့် STR လက်ခံရရှိမှု

၆ နေရာဒေသအလိုက် အွန်လိုင်းလိမ်လည်မှုနှင့်ဆက်နွယ်သည့် သံသယဖြစ်ဖွယ်လွှဲပြောင်းဆောင်ရွက်မှု သတင်းပို့ချက်(STR) လက်ခံရရှိမှု

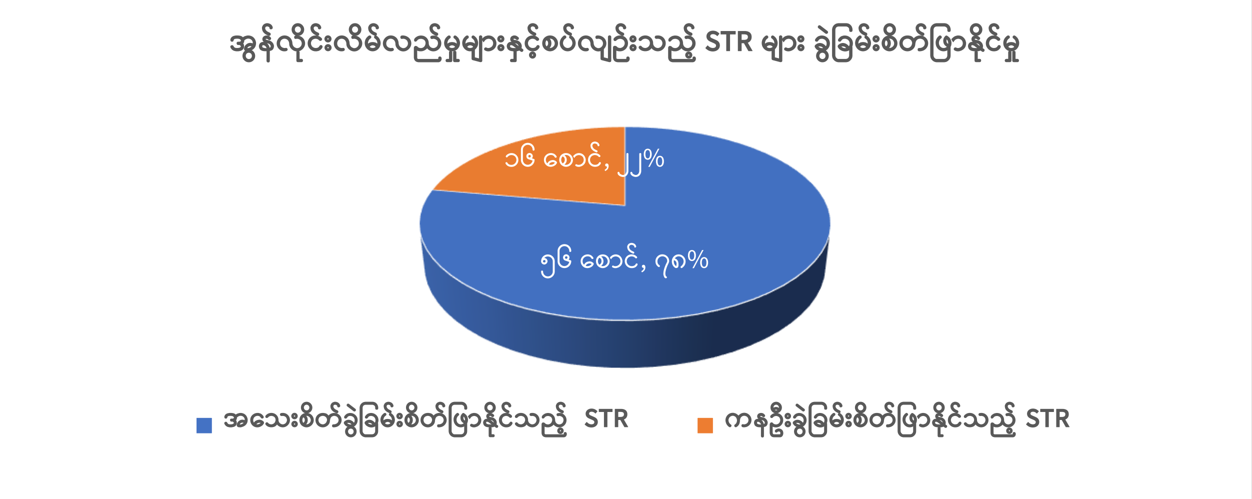
၇။ ၂၀၂၃ ခုနှစ်အတွင်း ငွေကြေးဆိုင်ရာစုံစမ်းထောက်လှမ်းရေးအဖွဲ့(FIU)က လက်ခံရရှိသည့် အွန်လိုင်း လိမ်လည်မှုနှင့်ဆက်နွယ်သော သံသယဖြစ်ဖွယ်လွှဲပြောင်းဆောင်ရွက်မှု သတင်းပို့ချက်(STR)များကို နေရာဒေသအလိုက် သတ်မှတ်ဆောင်ရွက်ရာတွင် ပေးပို့သူ(Conductor)၏ လွှဲပြောင်းဆောင်ရွက်မှုစတင်သည့် နေရာဒေသအပေါ် မူတည်၍ သတ်မှတ်ထားရှိပါသည်။ နေပြည်တော်ကောင်စီနယ်မြေ၊ တိုင်းဒေသကြီး/ပြည်နယ်(၁၅)ခုအနက် တိုင်းဒေသကြီး/ပြည်နယ်(၈)ခုမှ ပေးပို့လာခြင်း မရှိသည်ကို တွေ့ရှိရပါသည်။ STR ပေးပို့လာသည့် နေပြည်တော်ကောင်စီနယ်မြေအပါအဝင် တိုင်းဒေသကြီး/ပြည်နယ်(၇)ခုတွင် ရန်ကုန်တိုင်းဒေသကြီးသည် အများဆုံးပေးပို့ထားပြီး မန္တလေးတိုင်းဒေသကြီးနှင့် ရှမ်းပြည်နယ်တို့မှ ဒုတိယအများဆုံးပေးပို့ထားသည်ကို တွေ့ရှိရပါသည်။



ပုံ(၂) နေရာဒေသအလိုက် အွန်လိုင်း လိမ်လည်မှုနှင့်ဆက်နွယ်သည့် STR များ လက်ခံရရှိမှု

၇ အွန်လိုင်းလိမ်လည်မှုများနှင့်စပ်လျဉ်းသည့် Operational Analysis Report ဖြန့်ဝေနိုင်မှု

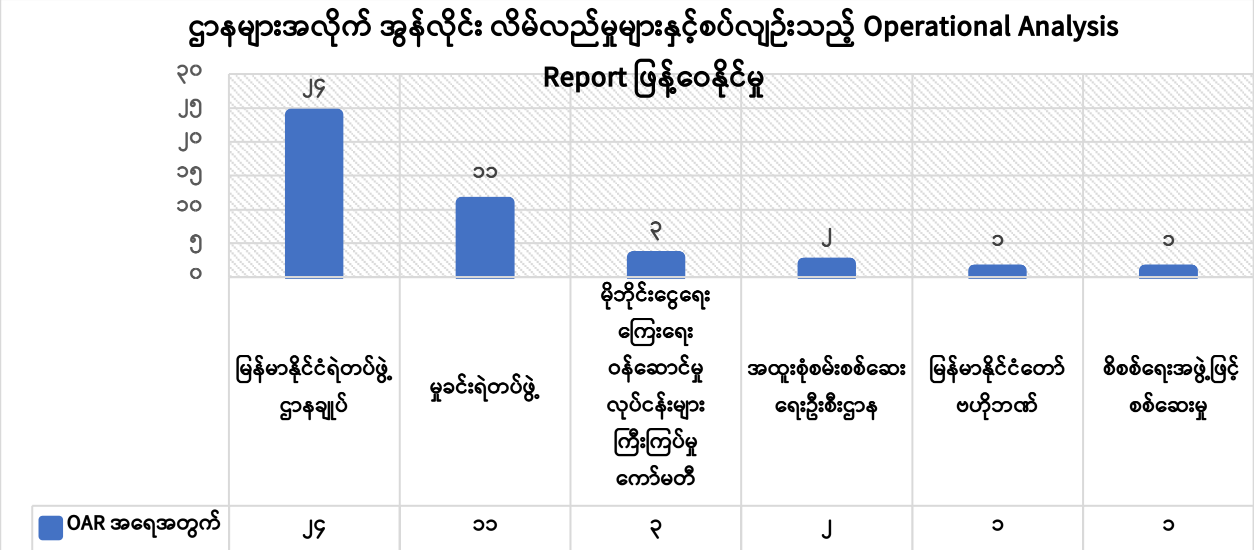
၈။ ငွေကြေးဆိုင်ရာ စုံစမ်းထောက်လှမ်းရေးအဖွဲ့(FIU)က လက်ခံရရှိသည့် အွန်လိုင်းလိမ်လည်မှုများနှင့်ဆက်နွယ်သည့် STR များအား လုပ်ငန်းနယ်ပယ်အလိုက်စိစစ်ခြင်း(Operational Analysis) ပြုလုပ်၍ တရားဥပဒေစိုးမိုးရေးအဖွဲ့အစည်း(LEA)များသို့ Operational Analysis Report (၂၂)စောင် ဖြန့်ဝေနိုင်ခဲ့ပါသည်။ Operational Analysis ဆောင်ရွက်ရာတွင် အွန်လိုင်းလိမ်လည်မှုနှင့် ဆက်နွယ်သည့် STR (၅၆)စောင်အား အသေးစိတ်ခွဲခြမ်းစိတ်ဖြာနိုင်ခဲ့ပြီး ၂၀၂၃ ခုနှစ် တစ်နှစ်တာကာလအတွင်း လက်ခံရရှိသည့် အွန်လိုင်း လိမ်လည်မှုများနှင့်ဆက်နွယ်သည့် STR စုစုပေါင်း(၇၂)စောင်နှင့် နှိုင်းယှဉ်ပါက ၇၈ % အသေးစိတ်ခွဲခြမ်းစိတ်ဖြာနိုင်ခဲ့သည်ကို တွေ့ရှိရပါသည်။



ပုံ(၃) အွန်လိုင်း လိမ်လည်မှုများနှင့်စပ်လျဉ်းသည့် Operational Analysis Report ဖြန့်ဝေနိုင်မှု

၈ ဌာနများအလိုက် အွန်လိုင်းလိမ်လည်မှုများနှင့်စပ်လျဉ်းသည့် Operational Analysis Report (OAR) ဖြန့်ဝေနိုင်မှု

၉။ အွန်လိုင်းလိမ်လည်မှုများနှင့်စပ်လျဉ်းသည့် OAR (၂၂)စောင်အား အစိုးရဌာန၊ တရားဥပဒေစိုးမိုးရေးအဖွဲ့အစည်း(၆)ခုသို့ ဖြန့်ဝေနိုင်ခဲ့ပါသည်။ ဌာနအလိုက်ဖြန့်ဝေမှုအား အောက်ဖော်ပြပါ ပုံတွင် ဖော်ပြထားရှိပါသည်။



ပုံ(၄) ဌာနများအလိုက် အွန်လိုင်း လိမ်လည်မှုများနှင့်စပ်လျဉ်းသည့် Operational Analysis Report ဖြန့်ဝေနိုင်မှု

၄ ဖော်ထုတ်တွေ့ရှိရသည့် အွန်လိုင်းလိမ်လည်မှု နည်းလမ်းများ (CEF Typologies)

၁၀။ ငွေကြေးဆိုင်ရာအရေးယူဆောင်ရွက်ရေးအဖွဲ့(FATF)၏ ၂၀၂၃ ခုနှစ်၊ နိုဝင်ဘာလတွင် ထုတ်ပြန်ခဲ့သည့် "Illicit Financial Flows from Cyber-Enabled Fraud" အစီရင်ခံစာတွင် အွန်လိုင်းလိမ်လည်မှုများအား "Cyber-Enable Fraud-CEF" အဖြစ် ခေါ်ဆိုသတ်မှတ်ထားပြီး အမျိုးအစား(၆)မျိုး ဖော်ပြထားပါသည်။[2] ဤအစီရင်ခံစာတွင် ငွေကြေးဆိုင်ရာ စုံစမ်းထောက်လှမ်းရေးအဖွဲ့ (FIU)၏ လုပ်ငန်းနယ်ပယ်စိစစ်ခြင်း (Operational Analysis) လုပ်ငန်းစဉ်မှ ဖော်ထုတ်ရရှိသည့် အွန်လိုင်းလိမ်လည်မှု အမျိုးအစားများကို FATF က သတ်မှတ်ထားသည့် အွန်လိုင်းလိမ်လည်မှု (CEF)အမျိုးအစားများအတိုင်း ခွဲခြားဖော်ထုတ်ထားပါသည်။ လုပ်ငန်းနယ်ပယ်စိစစ်ခြင်း (Operational Analysis) လုပ်ငန်းစဉ်အရ အများဆုံးဖော်ထုတ်ရရှိသည့် နည်းလမ်းများမှာ အောက်ပါအတိုင်း ဖြစ်ပါသည် -

(က) **နည်းလမ်း(၁)။** Application များ၊ Website အတုများအသုံးပြု၍ သတင်းအချက်အလက်များရယူပြီး ငွေကြေးများလိမ်လည်ခြင်း။ (Phishing Fraud)

(ခ) **နည်းလမ်း(၂)။** ဘဏ်နှင့် ငွေရေးကြေးရေးအဖွဲ့အစည်းများ သို့မဟုတ် မိုဘိုင်းငွေကြေးဝန်ဆောင်မှု လုပ်ငန်းများ၏ ဝန်ထမ်းအယောင်ဆောင်၍ လူမှုကွန်ရက်နှင့် တယ်လီဖုန်းဆက်သွယ်မှုများမှ တစ်ဆင့်လိမ်လည်ခြင်း။ (Social Media and Telecommunication Impersonation Fraud)

(ဂ) **နည်းလမ်း(၃)။** အွန်လိုင်းပေါ်တွင် ခင်မင်ရင်းနှီးအောင် ပြုလုပ်၍ လိမ်လည်ခြင်း။ (Online Romance Fraud)

(ဃ) **နည်းလမ်း(၄)။** အရောင်းအဝယ်လုပ်ငန်းများ၊ ရင်းနှီးမြှုပ်နှံမှုလုပ်ငန်းများကို အကြောင်းပြု၍ လိမ်လည်ခြင်း။ (Online trading/ trading platform Fraud)

(င) **နည်းလမ်း(၅)။** အလုပ်အကိုင်အခွင့်အလမ်းများရရှိမည်ဟု အကြောင်းပြု၍ လိမ်လည်ခြင်း။ (Employment Scams)

၄.၁ နည်းလမ်း(၁)။ Application များ၊ Website အတုများအသုံးပြု၍ သတင်းအချက်အလက်များရယူပြီး ငွေကြေးများလိမ်လည်ခြင်း

၁၁။ ဤနည်းလမ်းမှာ အသုံးများသော နည်းလမ်းတစ်ခုဖြစ်ပါသည်။ လိမ်လည်သူများသည် ဘဏ်နှင့် ငွေရေးကြေးရေးအဖွဲ့အစည်းများ(FIs)အမှတ်အသားတံဆိပ်များ အသုံးပြုပြီး Facebook Page လွှင့်တင်၍ အခက်အခဲများအားကူညီကြောင်း Post တင်ထားပါသည်။ လာရောက်အကူအညီတောင်းခံသူများအား Link တစ်ခုချပေးကာ အသင့်ပြုလုပ်ထားသည့် Application အား Download ဆွဲစေပြီး ငွေစာရင်း (Account)နှင့် ပတ်သက်သည့် အချက်အလက်များ၊ User Name နှင့် Password များ

[2] https://www.fatf-gafi.org/en/publications/Methodsandtrends/illicit-financial-flows-cyber-enabled-fraud.html

ဖြည့်သွင်းစေခြင်းဖြင့် ငွေစာရင်း(Account)အား ထိန်းချုပ်ရယူလိုက်ပါသည်။ ထို့နောက် Account အတွင်းရှိ ငွေများကို လိမ်လည်သူများအသုံးပြုသည့် Account တစ်ခုခုသို့ လွှဲပြောင်းခြင်းဖြင့် ငွေကြေးများရယူခြင်းဖြစ်ပါသည်။ ထို့အပြင် ဝန်ဆောင်မှုလုပ်ငန်းတစ်ခုခုကို လူမှုကွန်ရက်စာမျက်နှာတွင် လွှင့်တင်ကြော်ငြာ၍ ၎င်းစာမျက်နှာ(Page)များသို့ ဆက်သွယ်လာပါက ဆက်သွယ်လာသူ၏ Viber သို့ Link ပေးပို့ပြီး အသင့်ပြုလုပ်ထားသည့် Application အား Download ဆွဲစေပါသည်။ အဆိုပါ Application တွင် ငွေစာရင်း (Account)နှင့် ပတ်သက်သည့် အချက်အလက်များ၊ User Name နှင့် Password များ ဖြည့်သွင်းစေခြင်းဖြင့် လိမ်လည်သူများက ငွေစာရင်း(Account)အား ထိန်းချုပ်ရယူပြီး ငွေကြေးများကို မိမိတို့ ငွေစာရင်းသို့လွှဲပြောင်းခြင်း၊ ငွေသားထုတ်ယူခြင်းဖြင့် ဆောင်ရွက်ကြပါသည်။

၁၂။ ထို့အပြင် လိမ်လည်သူများသည် ပထမဦးစွာ လိမ်လည်ခံရမည့်သူများ၏ ကိုယ်ရေးအချက်အလက်များကို အခြားသောနည်းလမ်းများဖြင့် စုံစမ်းရယူကြပါသည်။ ယင်းနောက် လိမ်လည်ခံရသူ ငွေစာရင်းဖွင့်လှစ်ထားသည့် ဘဏ် သို့မဟုတ် ငွေကြေးဝန်ဆောင်မှုလုပ်ငန်းတစ်ခု၏ အမည်နှင့် တံဆိပ်များကို အသုံးပြုကာ **"သင့်ပရိုဖိုင်ဒေတာတွင် အမှားအယွင်းများကြောင့် သင့်အကောင့်သို့ ငွေအဝင်အထွက် လွှဲပြောင်းခြင်းကို ငြင်းပယ်ခဲ့ကြောင်း၊ ဤနေရာ (Link)ကိုနှိပ်၍ သင်၏ ကိုယ်ရေးကိုယ်တာအချက်အလက်များကိုဖြည့်သွင်းပါ"** စသည်ဖြင့် ယုံကြည်စေရန် ရေးသားပြီး လိမ်လည်ခံရမည့်သူ၏ Email သို့ Email ပေးပို့ပါသည်။

၁၃။ အဆိုပါ Link အား နှိပ်၍ ဖွင့်ကြည့်မည်ဆိုပါက လိမ်လည်ခံရသူ Account ဖွင့်လှစ်ထားသည့် ဘဏ် သို့မဟုတ် ငွေကြေးဝန်ဆောင်မှုလုပ်ငန်းတစ်ခုခု၏ အမည်များ၊ အမှတ်တံဆိပ်များဖြင့် အတုပြုလုပ်ထားသည့် Website သို့ ရောက်ရှိသွားမည်ဖြစ်ပါသည်။ ယင်းနောက် User Name နှင့် Password ဖြည့်သွင်းရန်ပေါ်လာမည်ဖြစ်ပြီး လိမ်လည်ခံရသူက အချက်အလက်များ ဖြည့်သွင်းလိုက်မည်ဆိုပါက လိမ်လည်သူမှ Account အား ထိန်းချုပ်ရယူကာ ငွေကြေးများလွှဲပြောင်းထုတ်ယူသော နည်းလမ်းဖြစ်ပါသည်။

၁၄။ ထို့အပြင် မိမိတို့အသုံးပြုသော လက်ကိုင်ဖုန်း Viber များသို့ မိမိ၏ **"ငွေစာရင်း Account ရှိ ငွေများကို Deactivate လုပ်လိုက်ကြောင်း၊ မသင်္ကာမှုဖြင့်ပိတ်သိမ်းလိုက်ကြောင်း ဖြေရှင်းလိုပါက (၂၄)နာရီအတွင်း အောက်ပါ Link သို့ ဝင်ရောက်ဖြေရှင်းပါ"**ဟု Message များပို့ခဲ့ရာ မိမိတို့က စိုးရိမ်စိတ်ဖြင့် ထို Link အား နှိပ်၍ ဖွင့်ကြည့်ပါက ဝန်ဆောင်မှုလုပ်ငန်းတစ်ခုခု၏ အမည်များဖြင့် User Name, Password ဖြည့်သွင်းရန် ပေါ်လာမည်ဖြစ်ပြီး မိမိ၏ User Name, Password ဖြည့်သွင်းပေးလိုက်ပါက ဘဏ်ငွေစာရင်း(Account)အား ထိန်းချုပ်ကာ ငွေကြေးများလွှဲပြောင်းရယူခြင်းဖြစ်ပါသည်။

ဖြစ်စဉ်နမူနာ(၁)

၁။ Ms.Brown သည် Facebook စာမျက်နှာရှိ E-BIKE Limited Page တွင် ကြော်ငြာထားသည့် လျှပ်စစ်ဆိုင်ကယ်အား ဝယ်ယူလိုသဖြင့် ယင်း Page ၏ Messenger မှ ဆက်သွယ်ခဲ့ရာ ဝယ်ယူလိုပါက E-BIKE Application အား Download ပြုလုပ်ရန်နှင့် အချက်အလက်များ ဖြည့်သွင်းရန် ပြောကြားခဲ့သဖြင့် ၎င်း၏အမည်၊ ဖုန်းနံပါတ်၊ CC Mobile Banking Username နှင့် Password တို့အား ဖြည့်သွင်းခဲ့ကြောင်း၊ ယင်းသို့ဖြည့်သွင်းခဲ့ပြီးနောက် ၎င်း၏ငွေစာရင်း(Account)အတွင်းမှ စုစုပေါင်းငွေကျပ် ၈၁ သိန်းကျော်အား (၃)ကြိမ်ခွဲ၍ Ms.White ဆိုသူ၏ ငွေစာရင်း(Account)အတွင်းသို့ လွှဲပြောင်းလိမ်လည်ရယူခဲ့ကြောင်း စိစစ်တွေ့ရှိရပါသည်။

ဖြစ်စဉ်နမူနာ(၂)

၂။ Ms.A သည် အချိန်ပိုင်းအိမ်အကူ ခေါ်ယူလိုသဖြင့် Facebook စာမျက်နှာရှိ Shwe Cleaning Page သို့ ဆက်သွယ်ခဲ့ရာ Application အား Download ပြုလုပ်ရန်နှင့် CC Mobile Banking ၏ Username/ Password ဖြည့်သွင်းရန် ပြောကြားခဲ့သဖြင့် လုပ်ဆောင်ခဲ့ပြီးနောက် ငွေကျပ် ၈,၇၉၆,၀၀၀ အား (၄)ကြိမ်ခွဲ၍ အခြားငွေစာရင်း(Account)တစ်ခုသို့ လွှဲပြောင်းလိမ်လည်ရယူသွားကြောင်း စိစစ်တွေ့ရှိရပါသည်။

ဖြစ်စဉ်နမူနာ(၃)

၃။ Dr.k သည် ၎င်းအသုံးပြုလျက်ရှိသည့် E-mail သို့ H BANK အမည်ရှိ E-mail အကောင့်တစ်ခုမှ စာဝင်၍ ဖတ်ကြည့်ရာ “**သင့် ပရိုဖိုင် ဒေတာတွင် အချက်အလက်များ မှားယွင်းနေ၍ ညွှန်ကြားချက်အတိုင်း လိုက်နာပါ**” ဆိုသည့်စာသား တွေ့ရှိရသဖြင့် ၎င်းမှ အဆိုပါ Link အား နှိပ်ခဲ့ရာ H BANK Application ထဲသို့ ရောက်ရှိသွားပြီး ၎င်း၏ Username, Password အား ထည့်ကာ ငွေစာရင်း(Account)အား စစ်ဆေးကြည့်ရှုရာ အချက်အလက်များမှန်ကန်၍ Logout ပြုလုပ်ခဲ့ကြောင်း၊ ထိုနေ့ညပိုင်းတွင် ၎င်း၏ ငွေစာရင်း(Account)အား ပြန်လည်စစ်ဆေးခဲ့ရာ ငွေကျပ် ၄၀,၀၀၀,၀၀၀ အား Ms.Q ၏ ငွေစာရင်း(Account)အတွင်းသို့ လိမ်လည်လွှဲပြောင်းရယူထားသည်ကို စိစစ်တွေ့ရှိရပါသည်။

ဖြစ်စဉ်နမူနာ(၄)

၄။ ၂၀၂၃ ခုနှစ်၊ အောက်တိုဘာလ ၂၆ ရက်နေ့တွင် ရန်ကုန်မြို့၊ S အိမ်ရာ၌ ရုံးခန်းဖွင့်လှစ်ထားသည့် F Co.,Ltd အား ဝင်ရောက်စီးနင်းရှာဖွေခဲ့ရာ Mr.T အပါအဝင် တရားခံ(၈၈)ဦးကို လည်းကောင်း၊ H Condo တွင် နေထိုင်သူ ကွင်းဆက်တရားခံ(၇)ဦးကိုလည်းကောင်း ဖမ်းဆီးရမိခဲ့ပြီး တရားခံများအနေဖြင့် ပြည်ပနိုင်ငံသားများထံမှ ငွေကြေးများ လိမ်လည်ရယူနိုင်ရန်အတွက် ပစ်မှတ်များရှာဖွေစုဆောင်းခြင်း၊ ရရှိသည့် ပစ်မှတ်များ၏ ကိုယ်ရေးအချက်အလက်များရယူရန်အတွက် အဖွဲ့တစ်ဖွဲ့လျှင်(၁၀)ဦးခန့်စီဖြင့် အဖွဲ့ငယ်(၈)ဖွဲ့ ဖွဲ့စည်းထားရှိပြီး WhatsApp လူမှုကွန်ရက်မှတစ်ဆင့် ပစ်မှတ်များထံ အချက်အလက်များ ရယူလေ့ရှိကြောင်း၊ ရရှိသည့်အချက်အလက်များအား ငွေကြေးလိမ်လည်မည့်အခြားအဖွဲ့များထံသို့ ပြန်လည်ရောင်းချခြင်းများ ပြုလုပ်ခဲ့ကြောင်း စိစစ်တွေ့ရှိရပါသည်။[3]

[3] https://www.moi.gov.mm/news/46515

၉.၂ နည်းလမ်း(၂)။ ဘဏ်နှင့် ငွေရေးကြေးရေးအဖွဲ့အစည်းများ သို့မဟုတ် မိုဘိုင်းငွေကြေး ဝန်ဆောင်မှု လုပ်ငန်းများ၏ ဝန်ထမ်းအယောင်ဆောင်၍ လူမှုကွန်ရက်နှင့် တယ်လီဖုန်း ဆက်သွယ်မှုများမှ တစ်ဆင့်လိမ်လည်ခြင်း

၁၅။ ဤနည်းလမ်းသည် K-Pay၊ WavePay ကဲ့သို့သော မိုဘိုင်းငွေကြေးဝန်ဆောင်မှုလုပ်ငန်းများက အသုံးပြုသူ User များထံ One Time Password (OTP) Code ပေးပို့သည့်စနစ်ပေါ်တွင် အမြတ်ထုတ် အသုံးပြုသောနည်းလမ်းဖြစ်ပါသည်။ ၎င်းစနစ်မှာ Password မေ့နေသူ သို့မဟုတ် လက်ကိုင်ဖုန်း ပြောင်းလဲအသုံးပြုသူ User များအတွက် Account Login ဝင်ရောက်နိုင်စေရန် User ၏ လက်ကိုင် ဖုန်းထံ OTP Code နံပါတ် ပေးပို့သောစနစ်ဖြစ်ပါသည်။

၁၆။ ပထမဦးစွာ လိမ်လည်သူများသည် ဘဏ်၊ မိုဘိုင်းငွေကြေးဝန်ဆောင်မှုလုပ်ငန်း သို့မဟုတ် အခြားဝန်ဆောင်မှုလုပ်ငန်းတစ်ခု၏ ဝန်ထမ်းအဖြစ်ဟန်ဆောင်ပြီး လိမ်လည်ခံရမည့်သူထံသို့ ဖုန်းဖြင့် ဆက်သွယ်ကာ "ငွေသွင်း/ငွေထုတ်မှုများသည် မသမာသည့် နည်းစနစ်များတွေ့နေရသည့်အတွက် မေးသည့်အချက်အလက်များအား ဖြေကြားအတည်ပြုပေးရန်နှင့် အတည်မပြုပါက Account အတွင်းရှိ ငွေများအားလုံးကို ယာယီပိတ်ထားမည်ဖြစ်ပြီး Account အား အပြီးဖျက်သိမ်းသွားမည် ဖြစ်ကြောင်း၊ အတည်ဖြစ် မဖြစ်ကို လက်ကိုင်ဖုန်းသို့ ပို့ပေးသည့် OTP Code ကို ပြန်လည်ပေးပို့ ရမည်ဖြစ်ကြောင်း" စသည်ဖြင့် အကြောင်းအမျိုးမျိုးပြကာ OTP Code ပေးပို့ သို့မဟုတ် ပြောကြား လာစေရန် ယုံကြည်အောင်ဖြားယောင်းပြောဆိုပါသည်။

၁၇။ တစ်ချိန်ထဲမှာပင် လိမ်လည်ခံရသူ၏ K-Pay သို့မဟုတ် Wave Pay Account အား လိမ်လည်သူက ၎င်း၏ လက်ကိုင်ဖုန်းဖြင့် ဝင်ရောက်ပြီး forget password ရွေးချယ်လိုက်ရာ လိမ်လည် ခံရသူ၏ လက်ကိုင်ဖုန်းထံသို့ OTP Code ရောက်ရှိလာပါသည်။ လိမ်လည်ခံရသူက OTP Code အား ပေးပို့လာပါက လိမ်လည်သူများက Account အား ထိန်းချုပ်ရယူလိုက်ပြီး ၎င်းတို့၏ ငွေစာရင်းများထဲသို့ ငွေကြေးများလွှဲပြောင်းခြင်းဖြင့် လိမ်လည်ရယူသောနည်းလမ်းဖြစ်ပါသည်။

၁၈။ ထို့အပြင် မိုဘိုင်းငွေကြေးဝန်ဆောင်မှုလုပ်ငန်းများ၏ ဝန်ထမ်းဟန်ဆောင်၍ လိမ်လည်ခံ ရမည့်သူ၏ လက်ကိုင်ဖုန်းထံဆက်သွယ်ကာ ကံစမ်းမဲပေါက်ကြောင်း၊ OTP Code ပေးပို့မည် ဖြစ်ကြောင်း၊ ကံစမ်းမဲထုတ်ရန်အတွက် OTP Code အားပြန်လည် ဖြေကြားရန်လိုအပ်မည် ဖြစ်ကြောင်း ယုံကြည်အောင်ပြောဆို၍ OTP Code အား လိမ်လည်တောင်းခံပါသည်။ လိမ်လည် ခံရသူထံမှ OTP Code လက်ခံရရှိပါက Account အား ထိန်းချုပ်ပြီး ၎င်းတို့၏ ငွေစာရင်းများထဲသို့ လွှဲပြောင်းခြင်းဖြင့် ငွေကြေးများ ရယူသောနည်းလမ်းဖြစ်ပါသည်။

ဖြစ်စဉ်နမူနာ(၅)

Mr.B ၏ ဖုန်းမှ Ms.Tin ၏ဖုန်းသို့ဆက်သွယ်၍ Phone Bill (၅၀,၀၀၀)ကျပ် ကံစမ်းမဲပေါက်သည်ဟု လိမ်လည်ပြောကြားခဲ့ပြီး Ms.Tin ၏ CC Pay Wallet အကောင့်မှ Username, Password နှင့် ၎င်း၏ဖုန်းသို့ ဘဏ်မှပေးပို့သည့် OTP Code အမှတ်အား တောင်းယူခဲ့ကြောင်း၊ ထို့နောက် Ms.Tin ၏ CC Pay Wallet Account အတွင်းရှိ ငွေကျပ် ၃၆၀,၀၀၀ အား Mr.B ၏ CC Pay Wallet Account သို့ လွှဲပြောင်း လိမ်လည်ရယူသွားကြောင်း စိစစ်တွေ့ရှိရပါသည်။

၉.၃ နည်းလမ်း(၃)။ အွန်လိုင်းပေါ်တွင် ခင်မင်ရင်းနှီးအောင်ပြုလုပ်၍ လိမ်လည်ခြင်း

၁၉။ ဤနည်းလမ်းသည် လူမှုကွန်ရက်အသုံးပြုသူများကို ပစ်မှတ်ထားကျူးလွန်လေ့ရှိသော နည်းလမ်းဖြစ်ပါသည်။ လိမ်လည်သူများသည် ပထမဦးစွာ မိမိတို့အသုံးပြုသော Facebook Account များတွင် နိုင်ငံခြားသား/သူ ပုံများဖြင့် Profile ပြုလုပ်၍ လိမ်လည်ခံရမည့်သူအား Messengers၊ Viber ဖြင့် အပြန်အလှန်ဆက်သွယ်ကာ အကြောင်းအရာအမျိုးမျိုး၊ ပုံစံအမျိုးမျိုး ဇာတ်လမ်းဆင်ပြောဆိုပြီး ရင်းနှီးအောင် ပြုလုပ်ကြပါသည်။

၂၀။ ရင်းနှီးမှုရှိလာပါက မက်မောလောက်သည့် ငွေကြေး (ဒေါ်လာ) ပမာဏဖော်ပြ၍ အကြောင်းအမျိုးမျိုးပြကာ လက်ဆောင်အဖြစ် ပေးပို့လိုက်သည်ဟု ယုံကြည်အောင် လှည့်ဖြားပြောဆိုပါသည်။ ယင်းနောက် လက်ဆောင်များရောက်ရှိနေပြီး ထုတ်ယူရန် အခွန်ပေးဆောင်ရမည်ဟု အခြားသူတစ်ဦး အယောင်ဆောင်ကာ ငွေကြေးများလိမ်လည်တောင်းခံပါသည်။

၂၁။ ထို့အပြင် အွန်လိုင်းပေါ်တွင် ခင်မင်ရင်းနှီးလာပါက တန်ဖိုးကြီးပစ္စည်းများကို လက်ဆောင်ပေးလိုကြောင်း၊ တန်ဖိုးကြီးပစ္စည်းဖြစ်ကြောင်း၊ Delivery ကုမ္ပဏီဖြင့်ပို့လိုက်ကြောင်း ယုံကြည်အောင်ပြောဆို စည်းရုံးကြပါသည်။ ထို့နောက် Delivery ကုမ္ပဏီ၏ အမည်ဖြင့် လိမ်လည်ခံရမည့်သူ၏ လက်ကိုင်ဖုန်းသို့ ဆက်သွယ်ကာ "ပစ္စည်းရောက်ရှိကြောင်း၊ ပစ္စည်းရွေးရန်အတွက် ငွေလွှဲပေးရမည်ဖြစ်ကြောင်း၊ တန်ဖိုးကြီးပစ္စည်းအတွက် အခွန်ဌာနတွင် အကောက်ခွန်ငွေ ပေးဆောင်ရမည်ဖြစ်ကြောင်း၊ အဖိုးတန်ပစ္စည်းပါ၍ ဥပဒေနှင့်ညီညွတ်မှုမရှိသဖြင့် ဌာနဆိုင်ရာများသို့ ငွေကြေးပေးရမည်ဖြစ်ကြောင်း" စသည်ဖြင့် အကြောင်းအမျိုးမျိုးပြကာ ငွေကြေးများလိမ်လည်ရယူခြင်းဖြစ်ပါသည်။

ဖြစ်စဉ်နမူနာ(၆)

Ms.D သည် Facebook စာမျက်နှာမှတစ်ဆင့် အခြားနိုင်ငံတစ်ခုတွင် နေထိုင်သည်ဟု ဆိုသူ Mr.A နှင့် သိကျွမ်း ခဲ့ပါသည်။ ကာလအတန်ကြာပြီးနောက် Mr.A မှ Ms.D ထံသို့ ခရစ်မစတ်လက်ဆောင်အဖြစ် ဒေါ်လာ (၅၀,၀၀၀)ပေးပို့လိုက်ကြောင်း ပြောကြားခဲ့ပြီးနောက် Mr.Aung ဆိုသူမှ ဖုန်းဖြင့် ဆက်သွယ်၍ ခရစ်စမတ် လက်ဆောင်များရောက်ရှိနေကြောင်းနှင့် ထုတ်ယူရန်အတွက် အခွန်ပေးဆောင်ရမည်ဖြစ်ကြောင်း ပြောကြားခဲ့သဖြင့် Ms.D မှ မိတ်ဆွေဖြစ်သူ Ms.G ၏ ငွေစာရင်း Account ကို အသုံးပြု၍ Mr.Aung ၏ ငွေစာရင်းသို့ ငွေကျပ် ၉,၃၅၀,၀၀၀ အား (၂)ကြိမ်ခွဲ၍ လွှဲပြောင်းပေးခဲ့သော်လည်း ခရစ်စမတ်လက်ဆောင်ပေးပို့သည့်ဒေါ်လာများ ရရှိခြင်းမရှိဘဲ လိမ်လည်လွှဲပြောင်းရယူသွားခဲ့ကြောင်း စိစစ်တွေ့ရှိရပါသည်။

၉.၄ နည်းလမ်း(၄)။ အရောင်းအဝယ်လုပ်ငန်းများ၊ ရင်းနှီးမြှုပ်နှံမှုလုပ်ငန်းများကို အကြောင်းပြ၍ လိမ်လည်ခြင်း

၂၂။ ဤနည်းလမ်းမှာ လိမ်လည်သူများသည် Social Media Platform များပေါ်တွင် ကြော်ငြာအတုများ၊ ကုန်ပစ္စည်းအတုများလွှင့်တင်၍ ဟန်ပြရောင်းချကြပါသည်။ ဝယ်ယူသူများက ဆက်သွယ်လာပါက Delivery ဖြင့် ကုန်ပစ္စည်းများပေးပို့လိုက်ကြောင်း စာရွက်စာတမ်းအတုများ၊ ဘောင်ချာအတုများပြုလုပ်၍ ဝယ်ယူသူယုံကြည်စေရန် လှည့်ဖြားပါသည်။ ဝယ်ယူသူမှ ယုံကြည်ပါက ၎င်းတို့၏ ငွေစာရင်းများသို့ ငွေကြေးများလွှဲပြောင်းခိုင်းပြီး လိမ်လည်ရယူကြပါသည်။

၂၃။ ထို့အပြင် လူမှုကွန်ရက်တွင် ဟန်ပြ ကုမ္ပဏီများတည်ထောင်၍ ကြော်ငြာများလွှင့်တင်ပြီး အစုရှယ်ယာများရောင်းချ၍ ငွေကြေးများလိမ်လည်ရယူခြင်း၊ ဟန်ပြငွေကြေးဝန်ဆောင်မှုလုပ်ငန်းများတည်ထောင်၍ ကြော်ငြာများလွှင့်တင်ပြီး ငွေကြေးများလိမ်လည်ရယူကြပါသည်။

၂၄။ ထို့အပြင် လိမ်လည်သူများသည် ပထမဦးစွာ အင်တာနက်စာမျက်နှာ (Web page)များ လွှင့်တင်ထားပြီးနောက် လူမှုကွန်ရက်တွင် ခင်မင်ရင်းနှီးသူ (လိမ်လည်ခံရမည့်သူ(Victim)) အား ယင်းစာမျက်နှာတွင် Account ဖွင့်လှစ်အသုံးပြုစေရန် မက်လုံးပေး ဆွဲဆောင်ပါသည်။ Account ဖွင့်လှစ်ဝင်ရောက်ပြီးပါက ယင်းစာမျက်နှာတွင် ဖန်တီးထားသော ကုန်ပစ္စည်းမှာယူမှုများအား အော်ဒါတင်သွင်းခြင်းဖြင့် အမြတ်ငွေများရရှိနိုင်ကြောင်း၊ အမြတ်ငွေများကို သတ်မှတ်ထားသည့် အော်ဒါတင်သွင်းမှု အကြိမ်ရေပြည့်မှ ထုတ်ယူခွင့်ပြုကြောင်း မက်လုံးပေးဆွဲဆောင်ပါသည်။ သတ်မှတ်ထားသည့် အကြိမ်ရေပြည့်သော်လည်း ငွေကြေးများထုတ်ပေးခြင်းမပြုဘဲ လိမ်လည်ခြင်းဖြစ်ပါသည်။

ဖြစ်စဉ်နမူနာ(၇)

၁။ Ms.Su သည် UT ရတနာဆိုင်အမည်ရှိ Online Shop လုပ်ငန်းမှ စိန်ဝယ်ယူခဲ့ပြီး ဝယ်ယူခဲ့သည့် ပစ္စည်းတန်ဘိုးအား Ms.T ၏ ငွေစာရင်း(Account)အတွင်းသို့ ငွေကျပ် ၂,၄၁၀,၀၀၀ အား လွှဲပြောင်းပေးခဲ့သော်လည်း လက်ဝတ်ရတနာပစ္စည်းများ ပေးပို့ခြင်းမရှိဘဲ ငွေကြေးလိမ်လည်လွှဲပြောင်းရယူသွားကြောင်း စိစစ်တွေ့ရှိရပါသည်။

ဖြစ်စဉ်နမူနာ(၈)

၂။ Mr.A၊ ၎င်း၏ဇနီး Mrs.Q နှင့် Mr.B တို့သည် ZT Co.,Ltd ကို ထူထောင်ပြီး လူမှုကွန်ရက်(Facebook) တွင် THA ရင်းနှီးမြှုပ်နှံမှုကုမ္ပဏီအမည်ဖြင့် Page ဖွင့်လှစ်၍ အစုရှယ်ယာများခေါ်ယူခဲ့ပြီး ရင်းနှီးမြှုပ်နှံသူများထံ ပေးရန်ရှိသည့် အရင်းနှင့် အတိုးငွေစာရင်းများကို ပေးချေခြင်းမပြုဘဲ ထွက်ပြေးတိမ်းရှောင်၍ ငွေကြေးလိမ်လည်လွှဲပြောင်းရယူသွားကြောင်း စိစစ်တွေ့ရှိရပါသည်။

ဖြစ်စဉ်နမူနာ(၉)

၃။ Ms.K၊ Mr.A၊ Mr.B၊ Mr.C နှင့် Mr.D တို့သည် Facebook တွင် P Money Exchange နှင့် S Online Money Exchange အမည်ဖြင့် Page များ ထူထောင်၍ မြန်မာကျပ်ငွေနှင့် နိုင်ငံခြားငွေလဲလှယ်ဆောင်ရွက်ပေးကြောင်း ကြော်ငြာပြီး အမှန်တစ်ကယ်လဲလှယ်ပေးခြင်းမရှိဘဲ အုပ်စုဖွဲ့လိမ်လည်မှု ကျူးလွန်ကြောင်း စိစစ်တွေ့ရှိရပါသည်။

ဖြစ်စဉ်နမူနာ(၁၀)

၄။ Mr.T သည် လူမှုကွန်ရက်စာမျက်နှာ(FaceBook) တွင် Ms.P နှင့် ခင်မင်ရင်းနှီးခဲ့ပါသည်။ Ms.P မှ ၎င်းထံ GP အမည်ရှိ Website လိပ်စာပေးပို့လာပြီး ၎င်း Website တွင် အကောင့်ဖွင့်လှစ်ရန်နှင့် Website ရှိ ကုန်ပစ္စည်းအော်ဒါတင်ပေးရပြီး တစ်ရက်တာ ပစ္စည်းအော်ဒါတင်မှုအပေါ်တွင် အမြတ်ငွေ ရရှိကြောင်း၊ အမြတ်ငွေထုတ်ယူမှုအား အကြိမ်(၄၀)ပြည့်ပါက ထုတ်ယူရရှိကြောင်း ပြောဆိုစည်းရုံးလာပါ သည်။ Mr.T မှ GP အမည်ရှိ Website တွင် အကောင့်ဖွင့်လှစ်၍ ကုန်ပစ္စည်းအော်ဒါတင်သွင်းမှု များပြုလုပ်ခဲ့ပါသည်။ အော်ဒါတင်သွင်းမှုအကြိမ်(၄၀)မပြည့်မီ ယင်း Website မှ မကြာခဏ Luck Bonus ပေါက်သည်ဟုဆိုကာ Bonus ငွေများပေးလေ့ရှိပြီး ယင်း Bonus ငွေများထုတ်ယူလိုပါက ငွေထပ်မံ ပေးသွင်း ခိုင်းပါသည်။ Mr.T မှ အကြိမ်(၄၀)ပြည့်အောင် အော်ဒါတင်သွင်းခဲ့သော်လည်း ငွေများထုတ်ယူရရှိခြင်းမရှိဘဲ လိမ်လည်ခံခဲ့ရကြောင်း စိစစ်တွေ့ရှိရပါသည်။

၉.၅ နည်းလမ်း (၅)။ အလုပ်အကိုင်အခွင့်အလမ်းများရရှိမည်ဟု အကြောင်းပြ၍ လိမ်လည်ခြင်း

၂၅။ ဤနည်းလမ်းသည် လိမ်လည်သူများအနေဖြင့် Social Media Platform များပေါ်တွင် နာမည်ကြီး အလုပ်အကိုင်ရှာဖွေရေး Agency များ၏ တံဆိပ်အမှတ်အသားများကို အသုံးပြု၍ Web-page ထူထောင်ပြီး အလုပ်အကိုင်အတုများ၊ အလုပ်ခေါ်စာ(Demand Letter)အတုများဖြင့် လှည့်ဖြား ကမ်းလှမ်း၍ သင်တန်းတက်ရန် ငွေကြေးကြိုတင်တောင်းခံခြင်း၊ ဝန်ဆောင်ခကြိုတင် ကျသင့်ငွေများအား အကြောင်းအမျိုးမျိုးပြကာ တောင်းခံခြင်းဖြင့် လိမ်လည်လွှဲပြောင်းရယူသည့် နည်းလမ်းဖြစ်ပါသည်။ ၂၀၂၃ ခုနှစ်အတွင်း လက်ခံရရှိခဲ့သည့် STR များတွင် ယင်းနည်းလမ်း များဖြင့် ဆက်နွယ်၍ သံသယရှိသဖြင့် ပေးပို့လာသည့် STR များ မတွေ့ရှိရသော်လည်း Open Sources များအရ လိမ်လည်သူများအနေဖြင့် ဤနည်းလမ်းများကို အသုံးပြုကြောင်း တွေ့ရှိ ရပါသည်။

၉.၆ အခြားနည်းလမ်းများ

၂၆။ အွန်လိုင်းလိမ်လည်မှုနည်းလမ်းများအနက် အခြားကျူးလွန်လေ့ရှိသည့် နည်းလမ်းတစ်ခုမှာ တယ်လီဖုန်း SIM ကတ်များကို အသုံးပြုခြင်းဖြစ်ပါသည်။ လိမ်လည်သူများသည် ပစ်မှတ်(Victim)၏ နိုင်ငံသားစိစစ်ရေးကတ်၊ ဖုန်းနံပါတ်နှင့် ကိုယ်ရေးအချက်အလက်များကို တစ်နည်းနည်းဖြင့်ရယူကာ နိုင်ငံသားစိစစ်ရေးကတ်အတုပြုလုပ်ပြီး ဆက်သွယ်ရေးဝန်ဆောင်မှုလုပ်ငန်းများထံ “တယ်လီဖုန်း ပျောက်ဆုံးကြောင်း” အကြောင်းပြကာ Victim ၏ ဖုန်းနံပါတ်ပါသော SIM ကတ်အသစ်ကို လျှောက်ထားရယူပါသည်။ ထို့နောက် ဖုန်းနံပါတ်ဖြင့် ဖွင့်လှစ်ထားသော Victim ၏ Mobile Pay Account များကို ဝင်ရောက်၍ ငွေကြေးများအား မိမိတို့၏ Mobile Pay Account များသို့ လွှဲပြောင်းခြင်းဖြင့် ငွေကြေးများရယူကြပါသည်။ ထိုသို့ Victim ၏ Mobile Pay Account မှ ငွေကြေးများအား စတင်လွှဲပြောင်းရယူရာ၌လည်း နိုင်ငံသားစိစစ်ရေးကတ်အတုများဖြင့် ဖွင့်လှစ် ထားသည့် Account များကို အသုံးပြုကြပါသည်။

၁၀ အွန်လိုင်းလိမ်လည်မှုနှင့် ငွေကြေးခဝါချမှုအကြားဆက်နွယ်မှု

၂၇။ အွန်လိုင်းလိမ်လည်မှုဆိုသည်မှာ အင်တာနက်ဆက်သွယ်ရေးကို အခြေခံသည့် ငွေကြေးဝန်ဆောင်မှုလုပ်ငန်းများ၊ လူမှုကွန်ရက်စာမျက်နှာများ (Facebook၊ Telegram၊ Viber စသည်ဖြင့်)နှင့် အင်တာနက်စာမျက်နှာ(Website)များအပြင် တယ်လီဖုန်းဆက်သွယ်မှုကွန်ရက်များကို တလွဲအသုံးပြု၍ ငွေကြေးအကျိုးအမြတ်များရရှိစေရန် လိမ်လည်ခြင်းဖြစ်ပါသည်။

၂၈။ သို့ဖြစ်ရာ အွန်လိုင်းလိမ်လည်မှုကျူးလွန်ရာတွင် ငွေကြေးလွှဲပြောင်းဆောင်ရွက်ရာ၌ Mobile Banking နှင့် Mobile Pay ကဲ့သို့သော အင်တာနက်ဆက်သွယ်ရေးအခြေပြု ငွေကြေးဝန်ဆောင်မှုလုပ်ငန်းများကို မဖြစ်မနေအသုံးပြုရပါသည်။ ငွေကြေးများလွှဲပြောင်းရာ၌ ငွေကြေးစီးဆင်းမှု (Money Trail) ကို နောက်ကြောင်းလိုက်လံဖော်ထုတ်ခြင်း မခံရစေရန်နှင့် အကျိုးခံစားခွင့်ရှိသူပိုင်ရှင်(BO)ကို ဖုံးကွယ်နိုင်ရန်အတွက် ကြိုးပမ်းအားထုတ်လာရာမှ ငွေကြေးခဝါချမှုနှင့် ဆက်နွယ်လာပါသည်။ ဘဏ္ဍာရေးစနစ်၏ Digitalization အသွင်သို့ ပြောင်းလဲတိုးတက်လာမှုသည် လိမ်လည်မှုကျူးရာ၌ လိုအပ်သည့် ငွေကြေးလွှဲပြောင်းမှုများ၊ ဖုံးကွယ်မှုများအတွက် လျင်မြန်စွာလုပ်ဆောင်လာနိုင်စေပြီး ခဝါချရန်အတွက် အခွင့်အလမ်းများဖြစ်လာစေပါသည်။

၁၁ အခြားမှုခင်းများနှင့်ဆက်နွယ်မှု

၂၉။ ငွေကြေးခဝါချမှုအပြင် အွန်လိုင်းလိမ်လည်မှုသည် အခြားသောမှုခင်းများနှင့်လည်း ဆက်နွယ်နေပါသည်။ အများဆုံးဆက်နွယ်သည့်မှုခင်းများမှာ အွန်လိုင်းလိမ်လည်မှုကျူးလွန်ရာတွင် လိုအပ်သည့်သို့မဟုတ် မဖြစ်မနေဆောင်ရွက်ရသည့် စာရွက်စာတမ်းအတုပြုလုပ်မှုနှင့် ကိုယ်ရေးအချက်အလက်များရရှိရန် Hacking ပြုလုပ်ရသည့် ကွန်ပျူတာမှုခင်းများဖြစ်ပါသည်။

၃၀။ ထို့အပြင် အွန်လိုင်းလိမ်လည်မှုသည် လူမှောင်ခို/လူကုန်ကူးမှုများနှင့်လည်း ဆက်နွယ်နေပါသည်။ လိမ်လည်သူများသည် လူမှုကွန်ရက်စာမျက်နှာများတွင် အလုပ်အကိုင်ကြော်ငြာများလွှင့်တင်၍ သားကောင်(Victim) များအား လိမ်လည်ခေါ်ဆောင်ပြီး ရောက်ရှိလာပါက အွန်လိုင်းလိမ်လည်မှုလုပ်ငန်းများကို အတင်းအကြပ်စေခိုင်းခြင်းဖြင့် အွန်လိုင်းလိမ်လည်သည့်ဂိုဏ်း[4]များပေါ်ပေါက်လာပါသည်။ ထိုသို့ IT နည်းပညာကျွမ်းကျင်သူများနှင့် ဒေသ/နိုင်ငံ အသီးသီးမှ ဘာသာစကားမတူသော လူအမျိုးမျိုးကို မှောင်ခိုကူးကာ အတင်းအကြပ် စေခိုင်းခြင်းဖြင့် လိမ်လည်ခံရမည့်ပြစ်မှုတ်(Victim)များနှင့်စပ်လျဉ်းသည့် နယ်နိမိတ်အကန့်အသတ်များကို ကျော်လွှားနိုင်ကာ နိုင်ငံဖြတ်ကျော်ကျူးလွန်မှုများ ဖြစ်ပေါ်လာပါသည်။ အွန်လိုင်းလိမ်လည်ဂိုဏ်းများသည် လူကုန်ကူးမှုများနှင့် ဆက်နွယ်နေသည်ဖြစ်ရာ အများအားဖြင့် လက်နက်ကိုင်ပဋိပက္ခများဖြစ်ပွားသည့် နယ်စပ်ဒေသများတွင် ဖြစ်ပွားလေ့ရှိပါသည်။

---

[4] အွန်လိုင်းလိမ်လည်သည့်ဂိုဏ်းများကို တရုတ်ဘာသာစကားဖြင့် "ကျားဖြန့်" ဟုလည်း ခေါ်ဆိုသုံးနှုန်းကြပါသည်။

၁၂ အွန်လိုင်းလိမ်လည်ရာတွင် အသုံးပြုသည့် ငွေကြေးခဝါချမှုနည်းလမ်းများနှင့် လားရာများ

၃၁။ အွန်လိုင်းလိမ်လည်မှုဖြစ်စဉ်များတွင် လိမ်လည်မှု စတင်ကျူးလွန်သည့် အချိန်မှစ၍ နစ်နာသူ (Victim) ထံမှ ငွေကြေးများလွှဲပြောင်းလက်ခံရယူရာတွင် နောက်ကြောင်းလိုက်လံဖော်ထုတ်ခြင်းမှ ရှောင်ရှားနိုင်ရန်အတွက် ငွေကြေးခဝါချမှုနည်းလမ်းများ အသုံးပြုလာသည်ကို ဖော်ထုတ်တွေ့ရှိရပါသည်။ ငွေကြေးဆိုင်ရာစုံစမ်းထောက်လှမ်းရေးအဖွဲ့(FIU)၏ လုပ်ငန်းနယ်ပယ်စိစစ်ချက် (Operational Analysis)များအရ အောက်ပါငွေကြေးခဝါချမှုနည်းလမ်းများကို အွန်လိုင်းလိမ်လည်မှုကျူးလွန်ရာတွင် အများဆုံးအသုံးချလေ့ရှိသည်ကို တွေ့ရှိရပါသည် -

(က) နိုင်ငံသားစိစစ်ရေးကတ်အတုများဖြင့် ဖွင့်လှစ်ထားသည့် Bank Account နှင့် Mobile Pay Account များ အသုံးပြု၍ လိမ်လည်ခြင်း၊ လွှဲပြောင်းရယူခြင်း၊

(ခ) အွန်လိုင်းလိမ်လည်မှုကျူးလွန်ရာမှရရှိသည့် ငွေကြေး(POC)များကို ငွေသားဖြင့် ချက်ချင်းထုတ်ယူခြင်း၊ ချက်လက်မှတ်ဖြင့်ထုတ်ယူခြင်း၊ အခြားငွေစာရင်း (Account) များသို့ ထပ်မံလွှဲပြောင်းခြင်း၊

(ဂ) ငွေလွှဲ၊ ငွေထုတ်(Money Exchange)လုပ်ကိုင်သူ Agent များ၊ အမည်ခံငွေစာရင်း (Account)များ၊ Money Mule Account များကို ကြားခံအဖြစ် အသုံးပြု၍ လွှဲပြောင်းဆောင်ရွက်ခြင်း၊

(ဃ) သဏ္ဌာန်ဆောင်ကုမ္ပဏီကို အသုံးပြု၍ ငွေစာရင်း (Account)များ ဖွင့်လှစ်ပြီး လွှဲပြောင်းခြင်း။

၃၂။ အထက်ပါနည်းလမ်းများအပြင် အွန်လိုင်းလိမ်လည်သူများသည် လိမ်လည်ရာမှရရှိသည့် ငွေကြေးများကို တရားဝင်မှတ်ပုံတင်ထားခြင်းမရှိသည့် ငွေလွှဲလုပ်ငန်း(ဟွန်ဒီ)များကို အသုံးပြု၍ ပြည်ပသို့ လွှဲပြောင်းခြင်းများဆောင်ရွက်လာနိုင်ပါသည်။ အထူးသဖြင့် အွန်လိုင်းလိမ်လည်ဂိုဏ်းများ၏ နယ်နိမိတ်အကန့်အသတ်ကို ကျော်လွှားကာ ကျူးလွန်နိုင်စွမ်းကြောင့် နိုင်ငံဖြတ်ကျော်ငွေကြေးလွှဲပြောင်းရာ၌လည်း တရားမဝင်ငွေလွှဲလုပ်ငန်းများကို အသုံးပြုလာနိုင်ပါသည်။ ယင်းအပြင် အွန်လိုင်းလိမ်လည်ရာမှ ရရှိသည့် ငွေကြေးများအား Crypto Currency နှင့် အခြားသော Virtual Assets များအသွင်သို့ ပြောင်းလဲပြီး နိုင်ငံဖြတ်ကျော်လွှဲပြောင်းခြင်းများဖြင့် ဖုံးကွယ်လာနိုင်ပါသည်။

၃၃။ ထို့အပြင် နိုင်ငံတော်အစိုးရနှင့် အိမ်နီးချင်းနိုင်ငံများ၏ ပူးပေါင်းနှိမ်နင်းမှုများကြောင့် အွန်လိုင်းလိမ်လည်ဂိုဏ်းများလျော့နည်းသွားပြီး လိမ်လည်သူများသည် ပြည်တွင်းရှိ နိုင်ငံသားများအား သားကောင် (Victim) အဖြစ် ပစ်မှတ်ထားရွေးချယ်လာပါသည်။ သို့ဖြစ်ရာ ပြည်တွင်းရှိ ဘဏ်နှင့် ငွေရေးကြေးရေးအဖွဲ့အစည်းများ၊ ငွေကြေးဝန်ဆောင်မှုလုပ်ငန်းများမှာ အွန်လိုင်းလိမ်လည်မှုအတွက် တလွဲအသုံးပြုနိုင်ခြေမြင့်မားလာပါသည်။ လိမ်လည်မှုများတွင် အနည်းဆုံး ၃ ဦး ပါဝင်ကျူးလွန်လေ့ရှိရာ ဘဏ်အများအပြားတွင် ငွေစာရင်း Account အများအပြားဖွင့်လှစ်ခြင်း၊ အဆင့်ဆင့်ထပ်မံလွှဲပြောင်းခြင်းများဆောင်ရွက်လာနိုင်ပါသည်။

၁၃ သုံးသပ်တင်ပြချက်

၃၄။ အွန်လိုင်းလိမ်လည်မှုများသည် အင်တာနက်ဆက်သွယ်မှုကိုအခြေခံသည့် ငွေကြေးဝန်ဆောင်မှုလုပ်ငန်းများကို တလွဲအသုံးပြု၍ ကျူးလွန်ခြင်းဖြစ်ရာ ဘဏ်နှင့်ငွေရေးကြေးရေးအဖွဲ့အစည်းများအနေဖြင့် ဆက်သွယ်ဆောင်ရွက်သူအပေါ်အလေးထားစိစစ်ခြင်း(CDD)နှင့် လွှဲပြောင်းဆောင်ရွက်မှုအပေါ် စောင့်ကြည့်ခြင်း(Transaction Monitoring)လုပ်ငန်းများကို အလေးထားဆောင်ရွက်ရမည်ဖြစ်ပါသည်။ ထိုသို့ဆောင်ရွက်ရာတွင် အွန်လိုင်းလိမ်လည်မှုနှင့် ဆက်နွယ်သည့် လွှဲပြောင်းဆောင်ရွက်မှုများကို သိရှိနိုင်ရန်အတွက် ဆုံးရှုံးနိုင်ခြေအန္တရာယ်ညွှန်းကိန်း (Red-flag Indicators)များကို နားလည်သိရှိထားရန်လိုအပ်မည်ဖြစ်ပါသည်။ နောက်ဆက်တွဲ(ခ)

၃၅။ ထို့အပြင် ဘဏ်နှင့် ငွေရေးကြေးရေးအဖွဲ့အစည်းများအနေဖြင့် မိမိတို့ဖောက်သည်များ၏ Mobile Wallet/banking Account များလုံခြုံမှုရှိစေရန်အတွက် လုံခြုံရေးစနစ်မြှင့်တင်ခြင်း (ဥပမာ- လက်ဗွေ၊ မျက်ကြည်လွှာ၊ မျက်နှာပုံသဏ္ဍာန် သို့မဟုတ် အသံစနစ်ဖြင့် အတည်ပြုသည့် လုံခြုံရေးစနစ် ထည့်သွင်းခြင်း)များ ပြုလုပ်ရန်လိုအပ်ပါသည်။ လိမ်လည်သူများသည် အွန်လိုင်းလိမ်လည်မှုများပြုလုပ်ရာတွင် လိုအပ်သည့် ဘဏ်ငွေစာရင်း Account များ ၊ Mobile Pay Account များ ဖွင့်လှစ်ရာ၌လည်း နိုင်ငံသားစိစစ်ရေးကတ်အတုများ၊ စာရွက်စာတမ်းအတုများအသုံးပြု၍ ဖွင့်လှစ်ဆောင်ရွက်ကြသည်ဖြစ်ရာ သတင်းပို့အဖွဲ့အစည်းများအနေဖြင့် CDD လုပ်ငန်းများဆောင်ရွက်ရာတွင် နိုင်ငံသားစိစစ်ရေးကတ်နှင့် ဆက်စပ်စာရွက်စာတမ်းများကို တိုးမြှင့်စိစစ်ရန် လိုအပ်ပါသည်။

၃၆။ အွန်လိုင်းငွေကြေးလိမ်လည်သူများသည် ငွေကြေးများအား လျင်မြန်စွာလွှဲပြောင်းခြင်း၊ ငွေသားထုတ်ယူခြင်းများ ဆောင်ရွက်လေ့ရှိရာ လွှဲပြောင်းဆောင်ရွက်မှုများနှင့်စပ်လျဉ်း၍ သံသယဖြစ်ဖွယ်တွေ့ရှိပါက ငွေကြေးဆိုင်ရာစုံစမ်းထောက်လှမ်းရေးအဖွဲ့(FIU)ထံ အချိန်နှင့်တစ်ပြေးညီ ပေးပို့ရန်လိုအပ်မည်ဖြစ်ပါသည်။

၁၄ နိဂုံး

၃၇။ အချုပ်အားဖြင့်ဆိုသော် ငွေကြေးလွှဲပြောင်းဆောင်ရွက်ရာတွင် လွယ်ကူလျင်မြန်ချောမွေ့စေသည့် Mobile Banking နှင့် Mobile Pay ကဲ့သို့သော အင်တာနက်ဆက်သွယ်ရေးအခြေပြုငွေကြေးဝန်ဆောင်မှုလုပ်ငန်းများ ဖွံ့ဖြိုးတိုးတက်လာမှုသည် အွန်လိုင်းလိမ်လည်မှုအတွက် အခွင့်အလမ်းများဖြစ်ပေါ်စေပါသည်။ အွန်လိုင်းလိမ်လည်မှုများတွင် ငွေကြေးခဝါချသည့်နည်းလမ်းများကိုအသုံးပြု၍ လွှဲပြောင်းဆောင်ရွက်ခြင်းများပါဝင်လေ့ရှိရာ ဘဏ်နှင့်ငွေရေးကြေးရေးအဖွဲ့အစည်းများ၏ AML/CFT ဆိုင်ရာ ဆောင်ရွက်ရမည့်ဝတ္တရားများကို အလေးထားလိုက်နာဆောင်ရွက်ခြင်း၊ တရားဥပဒေစိုးမိုးရေးအဖွဲ့အစည်းများနှင့် ပူးပေါင်းဆောင်ရွက်ခြင်းဖြင့် အွန်လိုင်းလိမ်လည်မှုများကို အချိန်နှင့်တပြေးညီ တားဆီးကာကွယ်နိုင်မည်ဖြစ်ပါသည်။

ငွေကြေးဆိုင်ရာစုံစမ်းထောက်လှမ်းရေးအဖွဲ့(FIU)

နောက်ဆက်တွဲ(က)

၂၀၂၃ ခုနှစ်အတွင်း ငွေကြေးဆိုင်ရာစုံစမ်းထောက်လှမ်းရေးအဖွဲ့(FIU)က လက်ခံရရှိသည့် အွန်လိုင်းလိမ်လည်မှုနှင့်စပ်လျဉ်းသည့် STR ဆိုင်ရာ အချက်အလက်များ

စဉ်	အမျိုးအစား	အရေအတွက်	ရေတွက်ပုံ
၁	လက်ခံရရှိသည့် STR ပေါင်း	၁၀၉၂	စောင်
၂	လိမ်လည်မှုနှင့်ဆက်နွယ်သည့် STR လက်ခံရရှိမှုပေါင်း	၇၂	စောင်
၃	အသေးစိတ်ခွဲခြမ်းစိတ်ဖြာသည့် လိမ်လည်မှုနှင့်ဆက်နွယ်သည့် STR	၅၆	စောင်
၄	အသေးစိတ်ခွဲခြမ်းစိတ်ဖြာသည့် လိမ်လည်မှုနှင့်ဆက်နွယ်သည့် STR များထဲမှ တစ်စောင်လျှင်အများဆုံး လွှဲပြောင်းသည့် တန်ဖိုးပမာဏ	၈၈၈,၆၇၇,၀၅၀	ကျပ်
၅	အသေးစိတ်ခွဲခြမ်းစိတ်ဖြာသည့် လိမ်လည်မှုနှင့်ဆက်နွယ်သည့် STR များထဲမှ တစ်စောင်လျှင်အနည်းဆုံး လွှဲပြောင်းသည့် တန်ဖိုးပမာဏ	၂,၁၀၀	ကျပ်
၆	အသေးစိတ်ခွဲခြမ်းစိတ်ဖြာပြီး OAR ဖြန့်ဝေခဲ့သည့် လိမ်လည်မှုနှင့်ဆက်နွယ်သည့် STR များထဲမှ တစ်စောင်လျှင်အများဆုံး လွှဲပြောင်းသည့် တန်ဖိုးပမာဏ	၈၈၈,၆၇၇,၀၅၀	ကျပ်
၇	အသေးစိတ်ခွဲခြမ်းစိတ်ဖြာ၍ OAR ဖြန့်ဝေခဲ့သည့် လိမ်လည်မှုနှင့်ဆက်နွယ်သည့် STR များထဲမှ တစ်စောင်လျှင်အနည်းဆုံး လွှဲပြောင်းသည့် တန်ဖိုးပမာဏ	၉၈,၀၀၀	ကျပ်
၈	အသေးစိတ်ခွဲခြမ်းစိတ်ဖြာ၍ OAR ဖြန့်ဝေခဲ့သည့် လိမ်လည်မှုနှင့် ဆက်နွယ်သည့် STR များ၏ စုစုပေါင်း လွှဲပြောင်းမှုတန်ဖိုးပမာဏ	၁၃၅၆,၁၇၉,၄၅၀	ကျပ်

နောက်ဆက်တွဲ(ခ)

အွန်လိုင်းလိမ်လည်မှုနှင့်ဆက်နွယ်သည့် ငွေကြေးခဝါချမှုဆိုင်ရာ ဆုံးရှုံးနိုင်ခြေအန္တရာယ်ညွှန်းကိန်းများ

ငွေကြေးလွှဲပြောင်းရယူဆောင်ရွက်သည့် နည်းပုံစံများ

၁။ ငွေစာရင်း Account ဖွင့်လှစ်ပြီးနောက် တန်ဖိုးပမာဏကြီးမားသည့် သို့မဟုတ် တန်ဖိုးပမာဏနည်းပါးသည့် ငွေကြေးတန်ဖိုးလွှဲပြောင်းဆောင်ရွက်မှုများကို ဖွင့်လှစ်ခဲ့သည့် ငွေစာရင်း Account ၏ ရည်ရွယ်ချက်(အနေအထား)နှင့် ကိုက်ညီမှုမရှိလောက်အောင် အလျင်အမြန် သို့မဟုတ် ချက်ချင်း လွှဲပြောင်းဆောင်ရွက်ခြင်း။

၂။ ငွေစာရင်းအကောင့်၌ ငွေကြေး(ရန်ပုံငွေ)ပမာဏအတိုင်းအတာ တစ်ခုထိလက်ခံခဲ့ပြီးနောက် လက်ကျန်ငွေ လုံးဝမကျန်ရှိလောက်အောင် ငွေပမာဏအများအပြားကို ငွေသားအဖြစ် အလျင်အမြန် သို့မဟုတ် ချက်ချင်းထုတ်ယူဆောင်ရွက်ခြင်း သို့မဟုတ် လွှဲပြောင်းဆောင်ရွက်ခြင်း။

၃။ ငွေစာရင်းအကောင့်ပိုင်ရှင်၏ စီးပွားရေးလုပ်ငန်းအခြေအနေနှင့် မကိုက်ညီသည့် ပမာဏများပြားသည့် ငွေကြေးလွှဲပြောင်းဆောင်ရွက်မှုများကို မကြာခဏပြုလုပ်ခြင်း (ဥပမာ - နိုင်ငံတကာသို့ ငွေကြေးလွှဲပြောင်းဆောင်ရွက်ခြင်းများ ရုတ်တရက်ပြုလုပ်ခြင်း၊ နိုင်ငံရပ်ခြားရှိ ATM ငွေထုတ်စက်များတွင် ငွေပေးချေသည့်ကတ်များဖြင့် ငွေသားများထုတ်ယူခြင်း၊ နိုင်ငံရပ်ခြား တင်ပို့/ပေးပို့မည့် ငွေကြေးကဲ့သို့ တန်ဖိုးလွှဲပြောင်း ဆောင်ရွက်နိုင်သည့် Virtual Assets များ သို့မဟုတ် ကုန်ပစ္စည်းများကို ပမာဏအများအပြား ဝယ်ယူခြင်း သို့မဟုတ် လိုင်စင်မဲ့ငွေကြေးလွှဲပြောင်းဆောင်ရွက်မှုဝန်ဆောင်မှု ပေးနေသည့် လုပ်ငန်းများ၏ အကူအညီဖြင့် ငွေပေးချေခြင်းများ)။

၄။ ငွေကြေးခဝါချမှုဆိုင်ရာဆုံးရှုံးနိုင်ခြေအန္တရာယ်မြင့်မားသည့် ဒေသများသို့ ငွေကြေးများလွှဲပြောင်းပေးပို့ခြင်း သို့မဟုတ် အဆိုပါဒေသများမှ ငွေကြေးများ လွှဲပြောင်းစီးဝင်ရောက်ရှိလာခြင်း။

၅။ တည်ထောင်ထားသည့် အချိန်ကာလမကြာသေးသည့် ကုမ္ပဏီများအနေဖြင့် ငွေကြေးပမာဏများစွာကို မကြာခဏ လွှဲပြောင်းဆောင်ရွက်မှုများနှင့်/ သို့မဟုတ် အဆိုပါ ကုမ္ပဏီများ၏ အဓိကလုပ်ငန်းလုပ်ရှားဆောင်ရွက်မှုပုံစံများမှာ အကျိုးခံစားခွင့်ရှိသူပိုင်ရှင်၏ လုပ်ငန်းအကောင် အထည်ဖော်ဆောင်ရွက်မှုပုံစံများနှင့်ကိုက်ညီမှု မရှိခြင်း သို့မဟုတ် တိတိကျကျမရှိသည့် ဘေဘုယျဆန်ဆန် ရည်ရွယ်ချက်ဖြင့်သာ လုပ်ငန်းဆောင်ရွက်နေခြင်း။

၆။ အကျိုးခံစားခွင့်ရှိသူပိုင်ရှင်တစ်ဦးတစ်ယောက်ထံသို့ ငွေပမာဏ အနည်းငယ်ပေးချေမှု တစ်ကြိမ်ပြုလုပ်၍ အောင်မြင်ပြီးနောက် အဆိုပါအကျိုးခံစားခွင့်ရှိသူပိုင်ရှင်ထံသို့ပင် တန်ဖိုးပမာဏများပြားသည့် ငွေကြေးပေးချေမှုများကို အလျင်အမြန် ဆက်လက် လွှဲပြောင်းခြင်း။

၇။ လွှဲပြောင်းဆောင်ရွက်မှုများသည် ကိန်းပြည့်တန်ဖိုးပမာဏအတိုင်း ပမာဏအများအပြား သို့မဟုတ် အကြိမ်ရေအများအပြားဖြင့် ဆောင်ရွက်ခြင်းဖြစ်ပြီး ၎င်းမှာ Gift Card များဖြင့် ဝယ်ယူသည့် ပုံစံအတိုင်းဖြစ်နေခြင်း။

ဖောက်သည်၏ ငွေကြေးလွှဲပြောင်းမှုဆိုင်ရာ တောင်းဆိုချက်များနှင့် ဖော်ပြချက်များ

၁။ ဖောက်သည်သည် အရောင်းအဝယ်ကိစ္စအတွက် တစ်စုံတစ်ဦးထံ ငွေပေးချေရာတွင် ယခင်က လွှဲပြောင်းဆောင်ရွက်ဖူးခြင်းမရှိသည့် ငွေစာရင်း Account ထံ လွှဲပြောင်း ဆောင်ရွက်မှု တစ်ကြိမ်ပြုလုပ်ပြီးနောက် နောက်ထပ်ငွေပေးချေနိုင်ရန်အတွက် ချက်ချင်း လွှဲပြောင်းဆောင်ရွက်ပေးရန်တောင်းဆိုခြင်း၊ ယင်းမှာ ပထမအကြိမ် အောင်မြင်စွာ လွှဲပြောင်းဆောင်ရွက်ပြီးနောက် ထပ်မံလွှဲပြောင်းဆောင်ရွက်ရန် ကြိုးပမ်းခြင်းကဲ့သို့သော လိမ်လည်သူများ၏ ပြုလုပ်လေ့ရှိသည့်ပုံစံများနှင့် ကိုက်ညီနေခြင်း၊

၂။ တရားဝင်ငွေပေးချေမှုပုံစံမျိုးရှိသည့် ဖောက်သည်၏ ငွေပေးချေမှုဆိုင်ရာ တောင်းဆိုချက် များသည် ယခင်ကာလက အတည်ပြုထားရှိပြီးဖြစ်သည့် ငွေပေးချေမှုဆိုင်ရာ တောင်းဆိုချက် များနှင့် မတူညီသည့် နေရာဒေသများမှ ဘာသာစကား၊ အချိန်ကာလနှင့် ငွေပမာဏတို့ ပါရှိနေခြင်း။

၃။ ငွေကြေးလွှဲပြောင်းမှုဆိုင်ရာ တောင်းဆိုချက်များတွင် "အရေးကြီး" ၊ "လျှို့ဝှက်" သို့မဟုတ် "လျှို့ဝှက်ထိန်းသိမ်းရမည့်အကြောင်းအရာ" ကဲ့သို့သော သတ်မှတ်ထားရှိသည့် အမှတ် အသားများ၊ ခိုင်လုံသည့် အထောက်အထားများ သို့မဟုတ် ဘာသာစကားများ ပါဝင် နေခြင်း။

၄။ ဖောက်သည်မှ ပေးပို့တင်ပြသည့် ငွေကြေးလွှဲပြောင်းမှုဆိုင်ရာ ကျိုးကြောင်းပြသည့် စာများ၊ အီးမေးလ်များသည် ပြည့်စုံမှုမရှိခြင်း (ဥပမာ- စာလုံးပေါင်းနှင့်/ သို့မဟုတ် အရေး အသားသဒ္ဒါ မှားယွင်းနေခြင်းမျိုးကဲ့သို့ ဖြစ်ပါသည်)။

၅။ ငွေကြေးလွှဲပြောင်းရန် တောင်းဆိုချက်သည် သိရှိထားပြီးဖြစ်သည့် အကျိုးခံစားခွင့်ရှိသူ ထံသို့ တိုက်ရိုက်ပေးပို့ရန် တောင်းဆိုခြင်းမျိုးဖြစ်သော်လည်း အကျိုးခံစားခွင့်ရှိသူ၏ ငွေစာရင်းအချက်အလက်များသည် ယခင်အသုံးပြုခဲ့သည့် အချက်အလက်များနှင့် ကွဲလွဲ နေခြင်း။

၆။ ငွေကြေးလွှဲပြောင်းပေးရန် တောင်းဆိုချက်တွင် ဖော်ပြထားသည့် ငွေကြေးများ လက်ခံမည့် Account ပိုင်ရှင် အမည်သည် ငွေကြေးများလက်ခံမည့်သူ၏ ဘဏ်ရှိ ငွေစာရင်း Account ပိုင်ရှင် အမည်မှာ ကိုက်ညီမှုမရှိခြင်း။

၇။ ဘဏ်တစ်ခုရှိ ငွေစာရင်း Account တစ်ခုသို့ ငွေကြေးများလွှဲပြောင်းပေးရန် တောင်းဆိုရာ၌ ဖော်ပြထားသည့် Account ပိုင်ရှင် အမည်မှာ ယင်းငွေကြေးများလက်ခံမည့် ဘဏ်ရှိ ဖွင့်လှစ်ထားသည့် ငွေစာရင်း Account ပိုင်ရှင် အမည်နှင့် ကွဲလွဲနေခြင်း။

၈။ (ဆုံးရှုံးနိုင်ခြေအန္တရာယ်မြင့်မားသည့်ဒေသများတွင် တည်ထောင်ထားသည့်) ကုမ္ပဏီများ၏ အကူအညီဖြင့် ရင်းနှီးမြှုပ်နှံမှုများ၊ ငွေကြေးဆိုင်ရာထုတ်ကုန်များနှင့် စပ်လျဉ်း၍ ငွေပေးချေရန်ဆိုသည့် အကြောင်းပြချက်ဖြင့် (ရင်းနှီးမြှုပ်နှံသူများဟု ယူဆရသည့်) စီးပွားရေးလုပ်ငန်းလုပ်ကိုင်သည့် လူပုဂ္ဂိုလ်များက စီစဉ်ဆောင်ရွက်သည့် ငွေကြေးလွှဲပြောင်းဆောင်ရွက်မှုများ။

ငွေစာရင်း Account ပိုင်ရှင်၏ Profile နှင့်စပ်လျဉ်း၍ သံသယဖြစ်ဖွယ်အချက်များ

၁။ ငွေစာရင်း Account ပိုင်ရှင်သည် CDD ပြုလုပ်ခံရန် ဆန္ဒမရှိခြင်း၊ CDD ပြုလုပ်မခံခြင်း။

၂။ ငွေစာရင်း Account ပိုင်ရှင်သည် ၎င်း၏ ငွေစာရင်းကို ဖြတ်သန်းလွှဲပြောင်းသည့် ငွေကြေးများ၏ အရင်းအမြစ်ကို မသိရှိခြင်း သို့မဟုတ် ၎င်းမှ အခြားသူတစ်ဦး တစ်ယောက်အတွက် ဆောင်ရွက်သည်ဟု ပြောဆိုခြင်း။

၃။ ဖောက်သည် သည် လွှဲပြောင်းဆောင်ရွက်မှုနှင့် စပ်လျဉ်းသည့် ရည်ရွယ်ချက်၊ ပမာဏ၊ အကြောင်းအရာနှင့် သဘာဝများကို ပြည့်စုံလုံလောက်စွာ မသိရှိခြင်း သို့မဟုတ် လွှဲပြောင်းဆောင်ရွက်မှုနှင့် စပ်လျဉ်း၍ လက်တွေ့မဆန်သော၊ ရှုပ်ထွေးသော သို့မဟုတ် မကိုက်ညီသော ရှင်းပြချက်များကို ပေးခြင်း။ (၎င်းမှာ ဖောက်သည် သည် Money Mule[5] တစ်ယောက်အဖြစ် ဆောင်ရွက်နေသည်ကို သံသယဖြစ်စေပါသည်။)

ငွေစာရင်း Account အသုံးပြုသူ၏ identity နှင့်ဆက်နွယ်သည့် သံသယဖြစ်ဖွယ် အချက်များ

၁။ ငွေစာရင်း Account အသုံးပြုသူသည် ခိုးယူထားသော၊ အတုပြုလုပ် ထားသော သို့မဟုတ် ပြောင်းလဲထားသော အချက်အလက်များကို အသုံးပြုခြင်းဖြင့် ၎င်း၏ identity ကို ဖုံးကွယ်ရန်ကြိုးစားနေခြင်း။ (ဥပမာ - လိပ်စာ၊ ဖုန်းနံပါတ်၊ Email များကို ပြောင်းလဲခြင်း)

[5] Money Mule ဆိုသည်မှာ လိမ်လည်သူများ၏ အသုံးချခံနေရသည့် ရိုးသားသည့် ကြားခံလူပုဂ္ဂိုလ်ဖြစ်ပြီး ယင်းသို့ အသုံးချခံနေရခြင်းကို မသိလိုက်ဘဲ သဘောရိုးဖြင့် ဆောင်ရွက်ပေးသူကို ဆိုလိုပါသည်။

၂။ ငွေစာရင်း Account ဖွင့်လှစ်ပြီးနောက် E-mail လိပ်စာများ၊ ဖုန်းနံပါတ်များ စသည့် ဆက်သွယ်ရမည့် အချက်အလက်များကို မကြာခဏပြောင်းလဲနေခြင်း။

၃။ E-mail လိပ်စာသည် ငွေစာရင်း Account ပိုင်ရှင်၏ အမည်နှင့် ကိုက်ညီမှုမရှိခြင်း သို့မဟုတ် ငွေစာရင်း Account အများအပြားတွင် ၎င်း E-mail လိပ်စာအမည်နှင့် ဆင်တူသည့် လိပ်စာအများအပြားရှိနေခြင်း။ (ဥပမာ - johnsmith1@example.com, john.smith@example.com, jsmith@example.com စသည်ဖြင့်)

၄။ ငွေစာရင်း Account သို့ Online ဖြင့် Login ဝင်ရောက်ရာတွင် ကြိမ်ဖန်များစွာ ကြိုးပမ်းဆောင်ရွက်နေခြင်း၊ သတင်းအချက်အလက်များဖြည့်စွက်ရန် တုန့်ဆိုင်းနေခြင်း။

၅။ ငွေစာရင်း Account ဝင်ရောက်သည့် IP Address မှာ ငွေကြေးခဝါချမှုဆိုင်ရာဆုံးရှုံးနိုင်ခြေ အန္တရာယ်မြင့်မားသည့် နိုင်ငံ/ဒေသမှ ဖြစ်နေခြင်း။ VPN အသုံးပြုဝင်ရောက်ခြင်း။

၆။ အွန်လိုင်း Account တစ်ခုအတွင်းသို့ IP Address အမျိုးမျိုးဖြင့် ဝင်ရောက်နေခြင်း။

ငွေစာရင်း Account ပိုင်ရှင်အပေါ် သံသယဖြစ်စေသည့်အချက်များ

၁။ ဆက်သွယ်ဆောင်ရွက်သူ သို့မဟုတ် ဖောက်သည်အပေါ် မသင်္ကာဖွယ်ရာ အချက်အလက် အထောက်အထားများနှင့် တိုက်ဆိုင်စိစစ် တွေ့ရှိနေခြင်း။ ဥပမာ - ငွေစာရင်း Account သည် ယခင်က လိမ်လည်ခံရကြောင်း ပြောကြားထားသူ (Victim) ၏ Account ဖြစ်နေခြင်း၊ Mule Account ဖြစ်နေခြင်း သို့မဟုတ် ကိုယ်ရေးအချက်အလက်များကို ခိုးယူခံရကြောင်း ပြောကြားထားသူ၏ အချက်အလက်များကို အသုံးပြု၍ ဖွင့်လှစ်ထားသည့် Account ဖြစ်နေခြင်း။

၂။ အခြား ဘဏ်နှင့်ငွေရေးကြေးရေးအဖွဲ့အစည်းများက ငွေကြေးများလွှဲပြောင်းရာတွင် လိမ်လည်မှုနှင့်စပ်လျဉ်း၍ သံသယဖြစ်ဖွယ်လုပ်ဆောင်ချက်ကို တွေ့ရှိသဖြင့် လွှဲပြောင်းဆောင်ရွက်မှုကို ပြန်လည်ရုပ်သိမ်းသည့် ငွေစာရင်း Account များ ဖြစ်နေခြင်း။

၃။ လွှဲပြောင်းဆောင်ရွက်မှုတွင် ပါဝင်သည့် လူပုဂ္ဂိုလ် သည် FIU နှင့် LEA များက ဖြန့်ဝေသည့် သတင်းအချက်အလက်များတွင် ပါဝင်နေခြင်း။

နောက်ဆက်တွဲ(ဂ)

အတိုကောက်ဝေါဟာရများ

အတိုကောက်	အဓိပ္ပါယ်ဖွင့်ဆိုချက်
AML/CFT	Anti-Money Laundering / Countering the Financing of Terrorism ငွေကြေးခဝါချမှုနှင့်အကြမ်းဖက်မှုကိုငွေကြေးထောက်ပံ့မှုတိုက်ဖျက်ရေး
BO	Beneficial Owner အကျိုးခံစားခွင့်ရှိသူပိုင်ရှင်
CDD	Customer Due Diligence ဆက်သွယ်ဆောင်ရွက်သူအပေါ်အလေးထားစိစစ်ခြင်း
FATF	Financial Action Task Force ငွေကြေးဆိုင်ရာအရေးယူဆောင်ရွက်ရေးအဖွဲ့
FI	Financial Institutions ငွေရေးကြေးရေးအဖွဲ့အစည်းများ
LEA	Law Enforcement Agencies တရားဥပဒေစိုးမိုးရေးအဖွဲ့အစည်းများ
MFIU	Myanmar Financial Intelligence Unit ငွေကြေးဆိုင်ရာစုံစမ်းထောက်လှမ်းရေးအဖွဲ့
OAR	Operational Analysis Report လုပ်ငန်းနယ်ပယ်စိစစ်ချက်အစီရင်ခံစာ
POC	Proceeds of Crime ပြစ်မှုကျူးလွန်ရာမှရရှိသည့် ငွေကြေးနှင့်ပစ္စည်းများ
STR	Suspicious Transaction Report သံသယဖြစ်ဖွယ်လွှဲပြောင်းဆောင်ရွက်မှုသတင်းပို့ချက်

For more studies

- Strategic Analysis Report on Trade-Based Money Laundering
  https://www.mfiu.gov.mm/sites/default/files/document/files/MFIU%၂၀Strategic%၂၀Analysis%၂၀on%၂၀TBML%၂၈၂၀၂၃%၂၉%၂၈Myan%၂၉%၂၈Amend%၂၉.pdf
- Money Laundering Trends Related to Drugs Crime
  https://www.mfiu.gov.mm/sites/default/files/document/files/Drugs%၂၀Strategic%၂၀Reports%၂၈August%၂၉%၂၈Myn%၂၉%၂၈update%၂၉.pdf
- Review on Suspicious Transactions Reported by Banks
  https://www.mfiu.gov.mm/sites/default/files/document/files/Review%၂၀on%၂၀STR%၂၀Reported%၂၀by%၂၀Banks_၂၀၂၃%၂၀November_Myanmar%၂၀Version%၂၀-%၂၀AG.pdf
- Money Laundering Risk Assessment on Legal Person
  https://www.mfiu.gov.mm/sites/default/files/document/files/Legal%၂၀Person%၂၀Risk%၂၀Assessment%၂၀Report%၂၀%၂၈၂၇%၂၀Jan%၂၀၂၀၂၃%၂၉%၂၈Myanmar%၂၉.pdf
- National Strategy on Anti-Money Laundering and Financing of Terrorism
  https://www.mfiu.gov.mm/sites/default/files/document/files/The%၂၀National%၂၀Strategy%၂၀on%၂၀AML-CFT%၂၀၂၀၁၉-၂၀၂၃%၂၀%၂၈English%၂၀Version%၂၉.pdf

For more information

Myanmar Financial Intelligence Unit

www.mfiu.gov.mm

review.mfiu@gmail.com