БИЗНЕС ИМЭЙЛ ЗАЛИЛАН

ТИПОЛОГИЙН ТАЙЛАН 2021

МОНГОЛБАНК

САНХҮҮГИЙН МЭДЭЭЛЛИЙН

АЛБА

АГУУЛГА

1. ТАНИЛЦУУЛГА

Сүүлийн жилүүдэд цахимаар үйлдэгддэг төрөл бүрийн гэмт хэрэг болон цахимаар залилан үйлдэх явдал ихсэж байгаа бөгөөд үүнд санхүүгийн байгууллагууд, бизнес эрхлэгчид, хувь хүмүүс өртөж санхүүгийн болон сэтгэлзүйн хувьд их хэмжээний хохирол амсаж байна. Цахимаар үйлдэгддэг санхүүгийн гэмт хэргүүд болон залилан, луйврын гэмт хэргүүдээс хамгийн хурдацтай тархаж, ихээр үйлдэгдэж байгаа хэргүүдийн нэг нь бизнес имэйл залилан юм.

Бизнес имэйл залилан[1] нь цахим шилжүүлэг ашиглан хийгддэг залилангийн нэг төрөл бөгөөд зөвхөн АНУ-д гэхэд л сүүлийн таван жилийн хугацаанд бизнес имэйл залилангийн 78,000 гаруй тохиолдол бүртгэгдэж иргэд, аж ахуйн нэгжүүд нийт 12 тэрбум доллар алдаж хохирсон байна[2]. Энэ төрлийн залилан үйлдэгчид нь бизнес эрхлэгч байгууллага, хувь хүн, мэргэжлийн үйлчилгээ үзүүлэгчдийг онилж, тэдний албаны болон хувийн имэйл хаягт хууль бусаар нэвтэрдэг бөгөөд хуурамч төлбөрийн нэхэмжлэх, заавар эсвэл бусад чухал мэдээллийг илгээх замаар санхүүгийн залилан, луйвар үйлддэг. Тухайлбал, гэмт этгээдүүд залилахаар онилсон байгууллагын аль нэг газар, хэлтсээс, удирдах албан тушаалтнаас, эсвэл нийлүүлэгчээс юмуу гэрээ байгуулсан өөр байгууллагаас илгээж байгаа мэт харагдахаар хуурамч имэйлийг эрх бүхий ажилтан руу нь явуулж, төлбөр, мөнгийг өөрсдийн шууд болон шууд бусаар удирдаж, эзэмшдэг данс руу шилжүүлэх заавар, зааварчилгааг илгээдэг байна. Ингэхдээ тухайн нөхцөл байдлаас хамаарч хохирогчдыг дотоод эсвэл гадаад улс руу төлбөр, мөнгө шилжүүлэх заавар өгдөг аж. Гэмт этгээдүүд хохирогчдыг эрхэлж буй бизнесийн үйл ажиллагаанаас нь хамаарч сонгодог бөгөөд ихэвчлэн гадаад худалдаа эрхэлдэг, үл хөдлөх хөрөнгийн гүйлгээ хийдэг болон тогтмол гадаад шилжүүлгийн гүйлгээ хийдэг аж ахуйн нэгж, хувь хүмүүсийг онилж сонгодог байна.

Бизнес имэйл залиланг илрүүлэх, мэдээлэх, түүнээс урьдчилан сэргийлэх ажилд банк, санхүүгийн байгууллагууд чухал үүрэг гүйцэтгэх бөгөөд банк, санхүүгийн байгууллагын комплаенсын нэгж, бизнес/үйл ажиллагааны эрсдэл хариуцсан нэгж, цахим эрсдэлийн нэгж гэх мэт хариуцсан газар, нэгжүүд болон үйлчилгээний ажилтнууд мэдлэг, мэдээлэл, нэгдсэн ойлголттой байж харилцан уялдаатай, хамтран ажиллах нь зөвхөн бизнес имэйл залилан гэлтгүй бусад төрлийн санхүүгийн гэмт хэргээс урьдчилан сэргийлж, харилцагчийг болон өөрийн байгууллагыг аливаа болзошгүй эрсдэлээс хамгаалах ач холбогдолтой юм.

Бизнес имэйл залилангийн тоо, хохирлын хэмжээ гадаад улсуудад төдийгүй Монгол Улсад эрс нэмэгдэж байгаа бөгөөд энэ залиланд өртөж алдсан хөрөнгө, мөнгийг ихэнх тохиолдолд буцааж олж авч чадахгүй байх магадлал өндрөөс гадна санхүүгийн байгууллагууд болон бизнесийн байгууллага, хувь хүмүүст бодитой аюул занал, хохирол учруулж байгаатай холбогдуулан Санхүүгийн мэдээллийн албанаас бизнес имэйл залилангийн тухай, энэ төрлийн залилан луйвар ямар шинж тэмдэгтэй байдаг вэ, ямар арга хэлбэрээр яаж үйлддэгддэг талаар, энэ төрлийн залилангийн шинж тэмдэг илэрвэл ямар арга хэмжээ авах талаар ерөнхий мэдээлэл, ойлголт өгөх зорилгоор мэдээлэх үүрэгтэй этгээд, эрх бүхий бусад байгууллагуудад зориулан энэхүү типологийн тайланг гаргаж байна.

[1] Business E-mail Compromise (BEC)

[2] Federal Bureau of Investigation (FBI) Public Service Announcement, Business Email Compromise: The 12 Billion Dollar Scam, July 12, 2018, available at https://www.ic3.gov/media/2018/180712.aspx .

2. ЗОРИЛГО, БҮТЭЦ

Санхүүгийн мэдээллийн албанаас энэхүү типологийн тайланг мэдээлэх үүрэгтэй этгээд болон эрх бүхий бусад байгууллагуудын ажилтнуудад бизнес имэйл залилантай холбоотой мэдээлэл өгөх, шаардлагатай тохиолдолд холбогдох арга хэмжээг цаг алдалгүй авах мэдлэг, чадавхитай болгох зорилгоор боловсруулан гаргав.

Бизнес имэйл залилан үйлдэгддэг арга хэлбэр, типологи болон гарсан бодит жишээ кейсүүдээс харахад энэ төрлийн гэмт хэрэгтэй тэмцэх хамгийн үр дүнтэй арга зам бол шилжүүлгийн гүйлгээг маш түргэн шуурхай зогсоох, шилжүүлсэн мөнгийг дагаж хаана, хэнд хүрч байгааг олж мэдэх, холбогдох болон эрх бүхий байгууллагууд аль болох богино хугацаанд дараагийн арга хэмжээг авах явдал юм. Үүнтэй холбогдуулан мэдээлэх үүрэгтэй этгээд болон холбогдох бусад байгууллагууд дараах арга хэмжээг авах шаардлагатай бөгөөд дэлгэрэнгүй мэдээллийг типологийн тайлангийн дараагийн хэсгүүдээр өгөх болно:

(1) Мэдээлэх үүрэгтэй этгээдийн ажилтнууд бизнес имэйл залилангийн талаар ойлголт, мэдээлэлтэй болох, улмаар хууль бус шилжүүлгийн гүйлгээ хийгдэхээс өмнө таньж илрүүлэх, зогсоох арга хэмжээ авах;

(2) Мэдээлэх үүрэгтэй этгээд нь харилцагчийг бизнес имэйл залиланд өртсөн эсвэл энэ талаар мэдсэн даруйд, мөн харилцагч залиланд өртөн буруу шилжүүлгийн гүйлгээ хийснийг мэдмэгц хууль сахиулах байгууллага, Санхүүгийн мэдээллийн албанд мэдээлэх арга хэмжээ авах;

(3) Хууль сахиулах байгууллага болон Санхүүгийн мэдээллийн алба, гадаад улсын Санхүүгийн мэдээллийн албад хоорондоо хамтран ажиллаж, гэмт хэрэг үйлдэгдсэн даруйд буюу аль болох богино хугацааны дотор (72 цагийн дотор байвал сайн гэж үздэг) луйвардуулсан/залилуулсан мөнгө, хөрөнгийг хаашаа шилжүүлснийг олж тогтоох, царцаах, цаашлаад буцааж олж авах арга хэмжээ авах.

Энэхүү типологийн тайлан нь нийт 9 хэсгээс бүрдэх бөгөөд үүнээс хойшх хэсгүүдэд бизнес имэйл залилан гэж юу вэ, ямар арга хэлбэрээр үйлдэгддэг вэ, энэ төрлийн залилангийн түгээмэл типологи, жишээ, шинж тэмдгүүд ямар байдаг вэ, бизнес имэйл залилантай холбогдох эрсдэлийг хэрхэн удирдаж, ямар хариу арга хэмжээ авч болох вэ гэсэн асуудлуудын хүрээнд дэлгэрэнгүй мэдээлэл өгөх болно. Мөн илүү ойлгомжтой болгох үүднээс Монгол Улсад болон бусад улс орнуудад гарч байсан бодит кейс жишээ, тохиолдлоос түүвэрлэн танилцуулна.

3. БИЗНЕС ИМЭЙЛ ЗАЛИЛАН, ТҮГЭЭМЭЛ ТИПОЛОГИУД

Бизнес имэйл залилан (БИЗ) (Business E-mail Compromise (BEC)/CEO Fraud/Wire-Transfer Fraud) гэдэг нь гэмт этгээдүүд бизнес эрхлэгч байгууллага, хувь хүнээс хууль бус аргаар, цахим шилжүүлгээр мөнгө залилж авдаг санхүүгийн залилан юм. Олон нийтийг залилдаг маркетингийн луйвар, понзи схем гэх мэт бусад залилан, луйвраас ялгаатай нь БИЗ үйлдэгчид нь гол төлөв бизнесийн байгууллагын ажилтан, бизнес эрхлэгч хувь хүнийг онилж сонгон, харилцаа холбооны систем, имэйлд нь хууль бусаар нэвтэрч хууран мэхлэх, хуурамч мэдээлэл илгээх, хуурамч имэйл хаяг үүсгэн хуурамч нэхэмжлэх, заавар илгээх замаар бизнесийн байгууллага, хувь хүн, санхүүгийн байгууллагаар цахим мөнгөн шилжүүлэг хийлгүүлж мөнгө, хөрөнгө залилж авдаг.

БИЗ үйлдэж байгаа этгээдүүд нь онилсон хувь хүн эсвэл компанийн бизнес хамтрагч, нийлүүлэгч эсвэл тухайн компанийн гүйцэтгэх захирал, санхүү хариуцсан захирал, мөнгөн шилжүүлгийн гүйлгээ хийх зөвшөөрөл олгох эрх бүхий ажилтан, албан тушаалтны дүр эсгэн, тэдний өмнөөс имэйл болон харилцаа холбооны бусад сувгийг ашиглан харилцаж, наанаа хууль ёсны юм шиг харагдах боловч зөвшөөрөлгүй, хууль бус гүйлгээний заавар өгдөг. БИЗ-ийн төрлүүд нь хоорондоо ялгаатай байх боловч бүгд бизнес эрхлэгч байгууллага, хувь хүн эсвэл санхүүгийн байгууллагыг төөрөгдүүлэн зөвшөөрөлгүй, хуурамчаар нэхэмжилсэн төлбөр тооцоог шилжүүлүүлэх, эсвэл тэднээр нууц мэдээллийг зөвшөөрөлгүй гуравдагч этгээдэд илгээлгэн, санхүүгийн луйвар, залилан хийдгээрээ ижил төстэй. Энэ төрлийн залилан, луйврын үед тохиолддог түгээмэл нэг шинж тэмдэг бол үг үсгийн болон зөв бичих дүрмийн алдаатай захидал, имэйлүүд байдгийг анхаарах хэрэгтэй.

Сошиал инженеринг[3] нь гэмт этгээдүүдийг БИЗ үйлдэх боломжийг олгодог үндсэн механизм юм. Европолийн үзэж байгаагаар сошиал инженеринг хэдий чинээ сайн байх тусам хохирогчийг залилах үйл ажиллагаа амжилттай болох магадлал төдий чинээ өндөр байдаг байна.

Сошиал инженеринг хийх үе шатууд

[3] Сошиал инженеринг (Social engineering) гэж хүний оролцоотойгоор янз бүрийн цахим халдлага, хор хөнөөлтэй ажиллагаа явуулахыг хэлнэ. Сошиал инженерингийн үед хэрэглэгчдийн сэтгэлзүйг төөрөгдүүлэх, хуурч мэхлэх замаар тэднээр нууц мэдээлэл гаргуулах, эсвэл сонор сэрэмжийг нь алдагдуулах аргыг ашигладаг байна.

БИЗ нь ерөнхийдөө дараах дөрвөн үе шатны дагуу үйлдэгддэг гэж үздэг байна. Үүнд:[4]

Нэгдүгээр үе шат: Хохирогчийг онилж, сонгох

Зохион байгуулалттай гэмт хэргийн бүлэглэл (гэмт этгээдүүд) бизнес эрхлэгчдийг онилж, интернетэд нээлттэй байгаа мэдээллийг ашиглан бизнес эрхлэгч хувь хүн, компани, түүний удирдлагууд, үйл ажиллагааных нь талаар болон тэдгээрийн бизнесийн хамтрагч, худалдан авагч талын мэдээллийг цуглуулна. Жил ирэх тусам гэмт этгээдүүдийн арга нарийсч байгаа бөгөөд гэмт этгээдүүд имэйл сервер дээрээс хэрэглэгчдийн имэйл хаягийг багцаар нь хууль бусаар олж авч, түлхүүр үгээр залилах хүн, компанийг онилж сонгох ч тохиолдол байдаг байна.

Хоёрдугаар үе шат: Хохирогч хувь хүн, компанийн мэдээлэл, имэйлд хууль бусаар нэвтрэх / хохирогчтой харилцаж ятгах

Гэмт этгээдүүд хохирогч хувь хүн, компанийн албаны эсвэл хувийн имэйл руу хууль бусаар нэвтрэх бөгөөд ингэхдээ ихэвчлэн тусгай програм, техник хэрэгсэл ашиглан хууль бусаар нэвтэрдэг байна. Үүний дараа гэмт этгээдүүд хохирогчийн имэйл болон өмнөх имэйл харилцаануудаас түүний санхүүгийн байгууллагын мэдээлэл, банк, дансны дэлгэрэнгүй мэдээлэл, байгуулсан гэрээ, худалдаа, төлбөр тооцооны мэдээлэл, холбоо барих хаяг, бусад холбогдох мэдээллийг олж авна.

[4] https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/business-email-compromise

Харин утсаар харилцаж залилах гэж байгаа тохиолдолд хохирогч компанийн албан тушаалтныг (ихэвчлэн санхүүгийн хэлтэст ажилладаг, гүйлгээ хийх эрх бүхий ажилтан, албан тушаалтан) сонгож утсаар ятгах, итгэл олж авах, эсвэл бүр дарамтлах зорилгоор нэг болон түүнээс олон удаа холбогдоно.

Гуравдугаар үе шат: Хуурамч гүйлгээ, төлбөр тооцооны мэдээлэл, заавар хүргүүлэх

Гэмт этгээдүүд хууль бусаар олж авсан мэдээллийг ашиглан хууль ёсны мэт харагдах төлбөр төлөх заавар, хүсэлтийг хохирогчийн санхүүгийн байгууллага руу имэйлээр илгээх эсвэл хохирогч руу нийлүүлэгч, бизнес хамтрагчийнх нь өмнөөс ирсэн мэт харагдахаар хуурамч имэйл, нэхэмжлэх илгээнэ. Ингэхдээ гэмт этгээдүүд хохирогчийн одоо ашиглаж байгаа жинхэнэ имэйл хаягийг ашиглах юмуу эсвэл жинхэнэ имэйлтэй нь төстэй хуурамч имэйл хаяг үүсгэж ашигладаг байна. Хууль ёсны мэт харагдуулах, улам үнэмшилтэй болгохын тулд гэмт этгээдүүд хуурамчаар үйлдсэн баримт бичиг нэмж хавсарган явуулж магадгүй.

Дөрөвдүгээр үе шат: Зөвшөөрөгдөөгүй гүйлгээ хийлгэх

Гэмт этгээдүүд хохирогч хувь хүн, компанийн ажилтан эсвэл санхүүгийн байгууллагыг хуурч мэхлэн, наанаа хууль ёсны мэт харагдаж байгаа боловч үнэндээ зөвшөөрөгдөөгүй, хийх ёсгүй мөнгөн шилжүүлэг хийлгүүлдэг. Энэ шатанд хохирогч өөрийгөө хууль ёсны бизнесийн гүйлгээ хийж байгаа гэдэгтээ итгэлтэй байна. Луйврын гүйлгээний заавар, нэхэмжлэх нь төлбөрийг гэмт этгээдүүдийн шууд болон шууд бусаар эзэмшдэг эсвэл удирддаг дотоод эсвэл гадаадын банк, санхүүгийн байгууллагад шилжүүлэх мэдээлэл, зааварчилгаа өгнө. Ингэхдээ гол төлөв зүүн, зүүн өмнөд Ази, баруун болон зүүн Европын орнуудад байрлах санхүүгийн байгууллагууд руу энэ төрлийн гүйлгээ хийх заавар өгдөг байна. Гэхдээ гэмт этгээдүүд өөрсдийн арга барил, гэмт хэрэг үйлдэх арга хэлбэрээ байнга өөрчилж байдаг тул дээр дурдсанаас өөр ямар ч улс руу хууль бус мөнгөн шилжүүлэг хийлгэж болохыг анхаарах нь зүйтэй.

Гэмт этгээдүүд хохирогчоор хуурамч цахим шилжүүлгийн гүйлгээг хийлгүүлэх буюу БИЗ-нг дээрх үе шатуудын дагуу үйлдэхдээ янз бүрийн арга, типологи ашигладаг байна. Үүнээс түгээмэл гурван арга, типологийг энд танилцуулья. Үүнд:

1. Имэйлд хууль бусаар нэвтэрч залилан үйлдэх

   Энэ төрлийн БИЗ нь санхүүгийн байгууллагууд болон тэдний үйлчлүүлэгчдийг хууль бусаар цахим шилжүүлэг хийлгүүлэх зорилгоор хуурамч эсвэл дууриалган нээсэн имэйл хаяг ашигладаг онцлогтой. Ингэхдээ БИЗ зохион байгуулагчид нь дор дурдсан арга техник ашиглаж санхүүгийн байгууллагуудын үйлчлүүлэгчдийг буюу хохирогчдыг онилж, хууран мэхэлдэг байна:

   (a) Компанийн эрх бүхий ажилтан харилцаж буй мэт харагдуулан, түүний имэйл хаягнаас компанийн данс байршиж байгаа банк, санхүүгийн байгууллага руу мөнгөн гуйвуулгын гүйлгээ хийх захиалга, хүсэлт өгч, шилжүүлэг хийхтэй холбоотой баримт бичгийг хавсарган явуулах;

(б) Компанийн бизнес түнш, нийлүүлэгч, эсвэл компанийн удирдлага харилцаж байгаа мэт болж, харахад хууль ёсны юм шиг хаягнаас имэйл бичиж гүйлгээ хийх заавар, нэхэмжлэхийг компанийн ажилтан руу илгээх, улмаар компанийн ажилтан уг имэйлийн дагуу гүйлгээ хийх;

(в) Брокер, нягтлан бодогч гэх мэт санхүүгийн мэргэжлийн үйлчилгээ үзүүлэгчийн имэйл хаягийг хуурамчаар, маш төстэйг дуурайлган нээж, үйлчлүүлэгчийнх нь нэрийн өмнөөс үйлчлүүлэгчийн банк эсвэл үнэт цаасны компани руу имэйл бичин, үйлчлүүлэгчийн данснаас мөнгийг гэмт этгээдүүдийн өөрсдийн эзэмшдэг эсвэл удирддаг данс руу шилжүүлэх захиалга, заавар өгөх;

(г) Үл хөдлөх хөрөнгө зуучлагч (эсвэл үл хөдлөх хөрөнгө худалдан авч байгаа хувь хүн), эскроу компани эсвэл өмгөөлөгч гэх мэт мэргэжлийн үйлчилгээ үзүүлэгч байгууллага, хүний имэйл хаягийг хуурамчаар дууриалган нээж, төлбөрийн нэхэмжлэх, зааврыг өөрчилж илгээн, гэмт хэрэгтний хяналтанд байдаг дансанд мөнгө шилжүүлж авах.

2. Утсаар зохион байгуулалттай холбогдож залилан үйлдэх

Гэмт этгээдүүд компанийн гүйцэтгэх захирал, бизнесийн түнш, эсвэл мөнгө шилжүүлэх зөвшөөрөл өгөх эрх бүхий албан тушаалтны дүр эсгэн компанийн санхүүгийн газар, хэлтэс рүү утсаар ярьдаг байна. Тэд маш чухал гэрээг компанийн дээд удирдлагууд тохиролцсон, хийсэн тул төлбөрийг яаралтай шилжүүлэх шаардлагатай байгаа талаар мэдэгдэх бөгөөд гэрээ, гэрээний төлбөрийн талаарх мэдээлэл болон энэ яриа нууц байх ёстой гэх мэтээр ярьдаг аж.

Гэмт этгээдүүд онилж сонгосон компанийн бүтцийн талаар маш сайн мэдлэгтэй байх бөгөөд ярьж байгаа төлбөр, түүнийг тойрсон асуудлуудыг аль болох бодитой харагдуулах зорилгоор хуурамч бичиг баримт бүрдүүлж үзүүлдэг / өгдөг байна. Энэ тохиолдолд гэмт этгээдүүд ихэвчлэн бүлэг, баг болж ажиллах ба жишээ нь, нэг нь гүйцэтгэх захирал, нөгөө нь компанийн хуульч, нөгөө нь нотариатчийн дүрд хувирах гэх мэтээр хамтран ажилладаг байна.

Ийнхүү компанийн ажилтныг утасны цаанаас шилжүүлэг хийхийг ятгаж чадсаны дараа тэд гэрээ, гүйлгээг нууцлахыг хатуу анхааруулж шаардана. Ажилтан үүнийг хууран мэхлэлт гэдгийг мэдэхгүй тул компани нь залилангийн хохирогч болсноо ойлгох хүртэл олон хоног болдог байна. Зарим тохиолдолд энэ хооронд залилан мэхлэгчид нэмж гүйлгээ хийх оролдлого ч хийдэг байна. Европолоос гаргасан жишээнд БИЗ-ийн нэг хохирогч Азийн улс руу 140 гаруй гүйлгээг шилжүүлсэн талаар дурдсан бөгөөд гүйлгээ тус бүр 500,000 евро хүртэл дүнтэй байсан (ойролцоогоор 552,000 ам.доллар) байна. Энэ жишээний хохирогч болох санхүүгийн байгууллага нь "дөрвөн нүд[5]" зарчмыг үйл ажиллагаандаа ашигладаг байсан боловч нийт 70 сая евро залилуулжээ.

[5] Дөрвөн нүдний зарчим гэдэг нь бизнесийн гүйлгээг доод тал нь хоёр хүн хянаж, зөвшөөрөл олгодог байхыг шаарддаг зарчим юм. Энэ зарчим нь бизнесийн ажил гүйлгээний ил тод байдал, хяналтыг дэмждэг онцлогтой.

3. Хуурамч төлбөрийн нэхэмжлэх илгээж залилан үйлдэх

БИЗ үйлдэх энэ төрлийн арга нь бизнес эрхлэгч хувь хүн эсвэл компанийн эрх мэдэл бүхий ажилтан (ихэвчлэн санхүүгийн эсвэл нягтлан бодох бүртгэл хариуцсан газрын) руу хуурамч төлбөрийн нэхэмжлэх илгээн, их хэмжээний мөнгийг гэмт этгээдүүдийн эзэмшдэг банкны данс руу шилжүүлүүлэх замаар үйлдэгддэг. Хуурамч төлбөрийн нэхэмжлэх илгээх залиланг зохион байгуулалттай гэмт бүлэглэл үйлддэг бөгөөд хууль бусаар хөрөнгө, мөнгийг олж авах, угаах зорилгоор хоорондоо холбоотой компаниуд, хүмүүсийн бүлэглэл, бүтцийг бий болгосон байдаг байна.

Гэмт этгээдүүд компаниудын эсвэл компани, хувь хүмүүсүүдийн хоорондын цахим харилцаанд нэвтрэх, улмаар дундуур нь орж цахим харилцааг саатуулах нарийн арга хэрэгслийг ашигладаг. Тэд энэ аргыг ашиглан хоёр талын хоорондын харилцаа, бизнес, худалдааны талаарх нарийн мэдээллийг олж авна. Ихэнх тохиолдолд гэмт этгээдүүд ийнхүү олж авсан мэдээллийг ашиглан хуурамч төлбөрийн нэхэмжлэх үйлдэж, уг нэхэмжлэхээ 1 дэх типологид заасны дагуу хуурамч буюу дууриалган нээсэн имэйлээр төлбөр төлөгч тал руу илгээх ба ихэвчлэн гэрээ, түүний хавсралт баримт бичиг, нэхэмжлэх дээрх төлбөр төлөх банк, дансны мэдээллийг өөрчлөн, хохирогчийн шилжүүлсэн хөрөнгө, мөнгийг өөрсдийн удирддаг, эзэмшдэг данс руу авдаг байна.

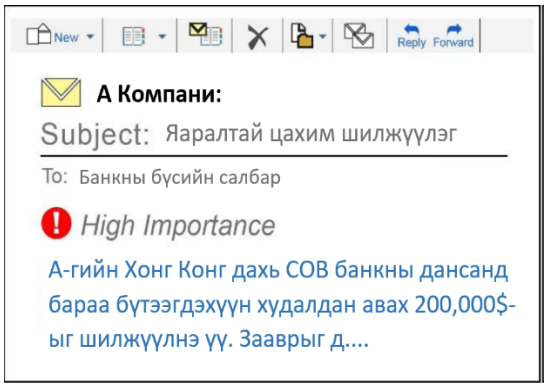
Гэхдээ гэмт этгээдүүд зөвхөн имэйл харилцаанд хууль бусаар нэвтэрч залилан үйлдээд зогсохгүй схемийг өөрчлөн үүнээс өөр хэлбэрээр ч залилан, луйвар үйлдэж болзошгүй.

4. БИЗНЕС ИМЭЙЛ ЗАЛИЛАНГИЙН ЖИШЭЭНҮҮД

БИЗ үйлдэгчид нь ихэвчлэн банк, санхүүгийн байгууллага, зээлийн үйл ажиллагаа эрхэлдэг байгууллага, үл хөдлөх хөрөнгийн компани, хуулийн фирмүүдээр дамжуулан өндөр дүнтэй, их хэмжээний гүйлгээ хийдэг бизнесийн байгууллагууд эсвэл тэдний үйлчлүүлэгчид, гадаад худалдаа болон бусад төрлийн бизнес эрхэлдэг компани, хувь хүмүүсийг онилдог. БИЗ-ийн түгээмэл жишээнүүдийг энд танилцуулья. Үүнд:

ЖИШЭЭ 1. Гэмт этгээд банк, санхүүгийн байгууллагын харилцагчийн дүр эсгэх:

Гэмт этгээд А компанийн санхүүгийн ажилтны имэйлд хууль бусаар нэвтэрч, имэйл хаягнаас нь А компанийн банк, санхүүгийн байгууллага руу мөнгө шилжүүлэх хуурамч гүйлгээний заавар, хүсэлт илгээнэ.[6] Энэ хүсэлтэд үндэслэн А компанийн банк, санхүүгийн байгууллага гүйлгээ хийж, гэмт этгээдүүдийн данс руу мөнгийг шилжүүлсэн байна.

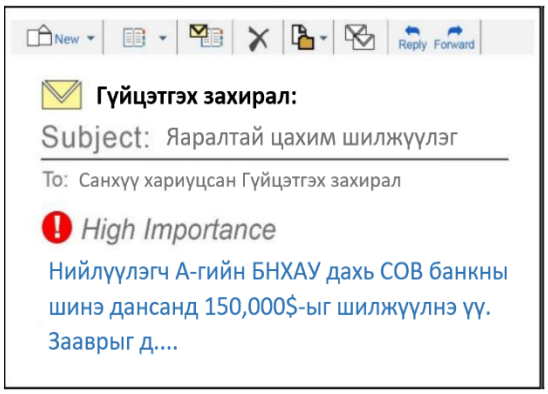


Энэ жишээн дээр гэмт этгээдүүд банк, санхүүгийн байгууллагын харилцагчийн дүр эсгэн тухайн банк, санхүүгийн байгууллагаар зөвшөөрөлгүй, хуурамч шилжүүлгийн гүйлгээ хийлгэж байна.

ЖИШЭЭ 2. Гэмт этгээд компанийн гүйцэтгэх удирдлагын дүр эсгэх:

Гэмт этгээд нь Б компанийн гүйцэтгэх удирдлагын имэйлд хууль бусаар нэвтэрч, имэйл хаягнаас нь компанийн гүйлгээг хийх эсвэл төлбөр тооцоог хариуцаж гүйцэтгэх үүрэгтэй ажилтанд шилжүүлгийн гүйлгээ хийх үүрэг даалгавар өгнө. Ийнхүү ажилтан гүйцэтгэх удирдлагын имэйлээр ирүүлсэн заавар, үүрэг даалгаврыг жинхэнэ буюу хууль ёсны гэж итгэн, Б компанийн банк, санхүүгийн байгууллагад зайнаас эсвэл биечлэн очиж гүйлгээ хийсэн байна.

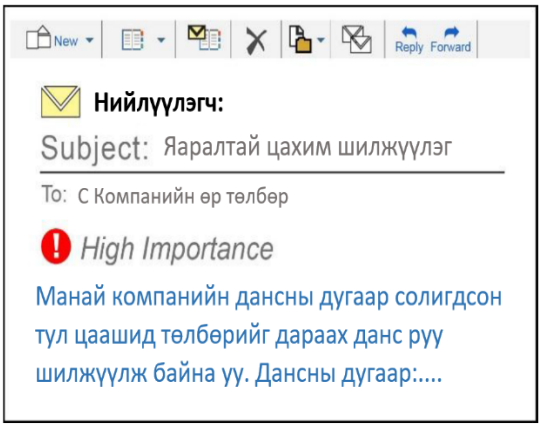
Энэ жишээн дээр компанийн гүйцэтгэх удирдлага болж дүр эсгэсэн гэмт этгээд нь компанийн ажилтныг зориудаар төөрөгдүүлэн мэхэлж, зөвшөөрөлгүй, хуурамч гүйлгээ хийлгэн, гэмт этгээдийн эзэмшдэг, удирддаг данс руу мөнгө шилжүүлүүлж байна. Энэ хувилбараас гадна компанийн гүйцэтгэх удирдлага болж дүр эсгэсэн гэмт этгээд нь компанийн ажилтныг төөрөгдүүлэн цалингийн мэдээлэл, гэрээ, төлбөр тооцооны мэдээлэл, гүйлгээний мэдээлэл гэх мэт чухал, нууц мэдээллүүдийг олж аван, дараа нь санхүүгийн залилан үйлдэхдээ ашигладаг байна.



[6] Зарим тохиолдолд гэмт хэрэгтэн ажилтны имэйлийг хакердахын оронд имэйл хаягийг нь дууриалган төстэйг хуурамчаар, шинээр үүсгэж ашигладаг байна.

ЖИШЭЭ 3. Гэмт этгээд нийлүүлэгчийн дүр эсгэх:

Гэмт этгээд нь С компанийн ханган нийлүүлэгчдийн аль нэг эсвэл мэргэжлийн үйлчилгээ үзүүлэгч (үл хөдлөх хөрөнгийн зуучлагч, эскроу компани, өмгөөлөгч гэх мэт)-ийн имэйлд хууль бусаар нэвтэрч, имэйл хаягнаас нь В компани руу имэйл илгээн тодорхой шалтгаан дурдаж, цаашид төлбөр тооцоо, нэхэмжлэхийн төлбөрийг имэйлд дурдсан банк, санхүүгийн байгууллага, дансны дугаар (шинэ эсвэл өмнөхөөс өөр) руу шилжүүлж байх талаар мэдэгддэг байна. Энэхүү хуурамч мэдээлэлд үндэслэн В компани ханган нийлүүлэгчийнхээ банк, дансны мэдээллийг бүртгэл, системдээ шинэчлэн оруулж, төлбөр тооцоогоо имэйлээр ирүүлсэн данс руу буюу гэмт этгээдийн данс руу шилжүүлнэ.



Энэ жишээн дээр гэмт этгээд нь ханган нийлүүлэгч, үйлчилгээ үзүүлэгчийн дүр эсгэн, компанийн ажилтныг зориудаар төөрөгдүүлэн мэхэлж, буруу банк, дансны мэдээллийг илгээн, улмаар гэмт этгээдийн эзэмшдэг, удирддаг данс руу мөнгө шилжүүлүүлж байна.

ЖИШЭЭ 4. Гэмт этгээд үл хөдлөх хөрөнгийн үйлчилгээг онилж, ашиглах:

Гэмт этгээд нь үл хөдлөх хөрөнгийн төлбөрийн мэдээллийг олж авах, төлбөрийн мэдээллийг өөрчлөх, гүйлгээг өөр тийш шилжүүлүүлэх зорилгоор үл хөдлөх хөрөнгө зуучлагч эсвэл үл хөдлөх хөрөнгө худалдан авагч, борлуулагч хувь хүний имэйлд хууль бусаар нэвтэрнэ. Ингээд дараа нь гэмт этгээд үл хөдлөх хөрөнгө зуучлагчийн имэйл рүү хууль бусаар нэвтэрч, эскроу компани руу имэйл бичиж үл хөдлөх хөрөнгө зуучлагчийн хөрөнгө борлуулсан зуучлалын хөлс болох төлбөрийг гэмт этгээдийн данс руу шилжүүлэх нэхэмжлэх илгээж, шилжүүлэг хийлгэсэн байна.

Энэ жишээн дээр гэмт этгээд нь үл хөдлөх хөрөнгө зуучлагч эсвэл үл хөдлөх хөрөнгийн гүйлгээний аль нэг оролцогчийг зориудаар төөрөгдүүлэн мэхэлж, хуурамч төлбөрийн мэдээлэл илгээн, урьдчилгаа төлбөр эсвэл үл хөдлөх хөрөнгийн гүйлгээтэй холбоотой бусад төлбөр, мөнгийг гэмт этгээдийн эзэмшдэг, удирддаг данс руу шилжүүлүүлж авч байна.

5. БИЗНЕС ИМЭЙЛ ЗАЛИЛАНГИЙН ШИНЖ ТЭМДГҮҮД

БИЗ-нг илрүүлэх, таслан зогсоохын тулд банк, санхүүгийн байгууллагууд харилцагч, үйлчлүүлэгчдийн гүйлгээний мэдээлэл болох төлбөрийн баримт (төлбөрийн даалгавар), нэхэмжлэх эсвэл гэрээ болон бусад холбогдох баримт бичгийг сайтар шалгаж нягтлан, тухайн гүйлгээтэй холбогдох нөхцөл байдлыг харгалзан үнэлэх шаардлагатай.

БИЗ-тай холбоотой байж болзошгүй сэжигтэй шинж тэмдгүүдийг дор ангилан жагсаалаа. Доор жагсаасан шинж тэмдгүүдийн зарим нь хууль ёсны санхүүгийн үйл ажиллагаа байж болох тул банк, санхүүгийн байгууллагууд гүйлгээ, үйлдэл нь БИЗ-тай холбоотой, сэжигтэй байж болзошгүй гэж шууд үзэхээс өмнө эдгээр шинж тэмдгээс гадна харилцагчийн санхүүгийн гүйлгээ, үйл ажиллагааны түүх гэх мэт тухайн гүйлгээ, нөхцөл байдлтай холбогдох бусад баримт, мэдээллийг харгалзан үнэлэх нь зүйтэй. Хэрэв шаардлагатай гэж үзвэл харилцагчаас асуулт асуух, тайлбар, мэдээлэл авах, нэмэлт баримт бичиг шаардах гэх мэт харилцагч, гүйлгээг нарийвчлан таньж мэдэх арга хэмжээ авах хэрэгтэй.

5.1.Хохирогчийн дансны үйл ажиллагаатай холбоотой шинж тэмдгүүд

5.1.1. Сэжигтэй гүйлгээний ерөнхий шинж тэмдгүүд

- Банк, санхүүгийн байгууллагын харилцагч өмнө нь мөнгө шилжүүлж байсан хүн, хуулийн этгээд рүү дахин мөнгө шилжүүлж байгаа боловч хүлээн авагчийн дансны мэдээлэл өмнөхөөс өөрчлөгдсөн байх;

- Харилцагч өмнө нь харилцаж байгаагүй, гүйлгээ хийж байсан түүхгүй бөгөөд бизнесийн харилцаатай эсэх нь тодорхойгүй хүлээн авагч руу мөнгө, төлбөр шилжүүлэх эсвэл мөнгө шилжүүлэх төлбөрийн даалгавар имэйлээр ирүүлэх ба шилжүүлгийн дүн нь харилцагчийн өмнө нь өөр харилцагч руу шилжүүлж байсан төлбөрийн дүнтэй ойролцоо эсвэл их дүнтэй байх;

- Харилцагч нь нийлүүлэгч, бизнесийн хамтрагч байгууллага руу төлбөр шилжүүлэхдээ өмнө нь ашиглаж байгаагүй данс руу мөнгө шилжүүлсний дараа тэр даруй эсвэл тун удалгүй нэмж мөнгө шилжүүлэх хүсэлт тавих. БИЗ үйлдэгчид залилан үйлдэх үедээ хохирогч тэдний заль мэхэнд унаж, мөнгөө шилжүүлснийг мэдмэгц хохирогчийг залилуулж байгаагаа мэдээгүй байх хугацаанд дахин мөнгө шилжүүлж авахыг санаархдаг;

- Харилцагч төлбөр шилжүүлэх хүсэлт тавихдаа гүйлгээг эсвэл гүйлгээтэй холбоотой гэрээ, бусад баримт бичгийг “Яаралтай”, “Нууц”, “Маш нууц” гэх мэтээр танилцуулах;

- Харилцагч нь банк, санхүүгийн байгууллагад гүйлгээг шалгаж баталгаажуулах хангалттай хугацаагүй эсвэл боломжгүй нөхцөл байдал үүсгэн шилжүүлгийн гүйлгээ хийх эсвэл төлбөрийн даалгавар имэйлээр илгээх;

- Харилцагч нь өмнө нь хуурамч эсвэл залилангийн гүйлгээ хийгдэж байсан гэх бүртгэлтэй эсвэл өөр харилцагчдийн мөнгөө шилжүүлээд алдсан, залилуулсан гэх гомдолд дурдагдаж байсан гадаад улсын санхүүгийн байгууллага дахь данс руу шилжүүлгийн гүйлгээ хийх хүсэлт тавих;

- Харилцагчаас имэйлээр илгээсэн гүйлгээний заавар, хүсэлт нь харахад хууль ёсны юм шиг мөртлөө урьд өмнө илгээж байсан гүйлгээний зааврааас өөр хэл дээр өөрөөр бичигдсэн, өөр цаг хугацаа, мөнгөний дүнг агуулсан бол;

- Харилцагчийн ашигладаг имэйл хаягтай маш төстэй боловч үл ялиг өөр буюу нэг болон хэд хэдэн тэмдэгт нэмэгдсэн, хасагдсан, эсвэл өөрчлөгдсөн имэйл хаягнаас гүйлгээний заавар, хүсэлт ирүүлэх. Тухайлбал:

Жинхэнэ имэйл хаяг:	Хуурамч имэйл хаяг:
trade-chin@asd.com	trade_chin@asd.com trade-chin@asb.com

- Харилцагч байгууллагын дансаар гүйлгээ хийхээр шинээр итгэмжлэгдэн томилогдсон ажилтан эсвэл өмнө нь шилжүүлгийн гүйлгээ хийж байгаагүй, мөн хүсэлт илгээж байгаагүй итгэмжлэгдсэн этгээд банк, санхүүгийн байгууллагад гүйлгээний заавар, хүсэлт ирүүлэх;

- Харилцагчийн ажилтан эсвэл итгэмжлэгдсэн төлөөлөгч нь гүйцэтгэх захирал, өмгөөлөгч, эсвэл эрх бүхий этгээдээс ирүүлсэн зөвхөн имэйл харилцаанд үндэслэн банк, санхүүгийн байгууллагад харилцагчийн нэрийн өмнөөс гүйлгээний заавар, хүсэлт ирүүлэх. Ингэхдээ харилцагчийн ажилтан эсвэл итгэмжлэгдсэн төлөөлөгч нь имэйл илгээсэн гүйцэтгэх захирал, өмгөөлөгч, эсвэл эрх бүхий этгээдтэй холбогдож, мэдээллийг баталгаажуулах боломжгүй байгаагаа илэрхийлэх.

5.1.2. Өндөр эрсдэлтэй улс орон руу мөнгө шилжүүлэх

- Төлбөр, мөнгө хүлээн авагчийн данс нь оффшор бүс нутаг, компанид харьяалагдах эсвэл тухайн банк, санхүүгийн байгууллага болон эрх бүхий байгууллагаас өндөр эрсдэлтэй гэж тооцсон бүс нутагт байрлах санхүүгийн байгууллага руу шилжүүлгийн гүйлгээ хийгдэх.

5.1.3. Хуурамч нэхэмжлэх эсвэл баримт бичиг ашиглах

- Гэмт этгээдүүд хохирогч хүн, байгууллагын ажилтан руу гүйлгээ хийлгэхээр эсвэл хийлгэх гэж байгаа гүйлгээг баталгаажуулах, итгэл үнэмшил төрүүлэх зорилгоор хуурамч нэхэмжлэх эсвэл баримт бичгийг имэйлээр илгээдэг. Хуурамч нэхэмжлэх, баримт бичиг нь дүрс, бичиглэлийн өндөр чанартай байж болох бөгөөд тэр байтугай гэмт этгээдийн санхүүгийн байгууллага дахь данс руу мөнгө шилжүүлүүлэх зорилгоор өөрчилсөн жинхэнэ баримтууд ч байж болно.

5.2.Залилагч этгээдийн дансны үйл ажиллагаатай холбоотой шинж тэмдгүүд

5.2.1. Сэжигтэй гүйлгээний ерөнхий шинж тэмдгүүд

- Гэмт этгээдүүд залилан үйлдсэнийхээ дараа шилжүүлгээр авсан мөнгийг тэр даруй банк, санхүүгийн байгууллага дахь данснаасаа бэлнээр зарлагадаж авах, банк, санхүүгийн байгууллагаас шууд өөр тийш шилжүүлэх, эсвэл санхүүгийн байгууллага доторх өөр хэд хэдэн данс руу тараан шилжүүлдэг байна.

- Банк, санхүүгийн байгууллага өөрийн харилцагчийн дансанд шилжүүлгийн гүйлгээ хүлээн авах боловч шилжүүлгийн мэдээлэл дэх хүлээн авагчийн нэр нь данс эзэмшигчийн нэрнээс өөр байх. Энэ нь хохирогч бизнесийн хамтрагчийнх нь дүр эсгэж залилж байгаа гэмт этгээдүүдийн өгсөн данс руу төлбөр, мөнгө шилжүүлэхдээ залилуулж байгаагаа мэдэлгүй, бизнесийн хамтрагчийнх нь данс гэж бодон тэдний нэрийг бичдэгээс үүдэн гэмт этгээдүүдийн эзэмшиж, удирдаж байгаа дансны нэрээс зөрдөг байна. Иймд банк, санхүүгийн байгууллага өөрийн харилцагчийн өөр санхүүгийн байгууллагаас хүлээн авч байгаа шилжүүлгийн гүйлгээний хувьд дансны дугаар, данс эзэмшигчийн нэр зөрж байгаа тохиолдолд БИЗ явагдаж байж болзошгүйг анхаарах хэрэгтэй.

5.2.2. Шилжүүлгийн гүйлгээний дүн

- Харилцагчийн дансандаа хүлээн авч байгаа шилжүүлгийн гүйлгээний дүн нь тухайн харилцагчийн ажил, бизнесийн үйл ажиллагаа, дансны үйл ажиллагаа, орлогын байдалтай нийцэхгүй байх.

5.2.3. “Мөнгө дамжуулагч” ашиглах

- Хийж байгаа гүйлгээ болон ажил эрхлэлт, дансны үйл ажиллагаа, орлогын байдал нь нийцэхгүй байгаа бөгөөд шилжүүлгийн гүйлгээ хүлээн авмагц тэр даруй бэлнээр зарлагадан авдаг, үгүй бол өөр тийш даруй шилжүүлдэг харилцагчид байдаг. Иймхарилцагчдын хувьд гүйлгээний дүн, дансны үлдэгдэл нь тодорхой шалтгаангүй гэнэт өсөх, дансанд нь мөнгө шилжиж орж ирмэгц тэр даруй бэлнээр авдаг эсвэл богино хугацааны дотор буцаагаад өөр данс, банк, санхүүгийн байгууллага руу шилжүүлж байгаа нь БИЗ-ийн луйврын схемд “мөнгө дамжуулагч”[7]-ын үүрэгтэй оролцож байж болзошгүйг илтгэнэ. БИЗ үйлдэж байгаа гэмт этгээдүүдийн хувьд залилан, луйвар хийхдээ ихэвчлэн мөнгө дамжуулагчийг ашигладаг бөгөөд мөнгө дамжуулагч нь гэмт хэрэгтэн, гэмт хэргийн бүлэглэлүүдэд дундын зуучлагч, дамжуулагч болж ашиглагддаг. Ихэнх тохиолдолд мөнгө дамжуулагч нь гэмт этгээдүүдэд гэмт хэргийн замаар олсон хөрөнгө, мөнгийг нь хууль бусаар зөөвөрлөх, дамжуулах, авч өгөх зорилгоор ашиглагдаж байгаагаа мэддэггүй. Мөнгө

[7] Money mules буюу “Мөнгө дамжуулагчид” нь хууль бус үйл ажиллагаа явуулж, гэмт хэрэг үйлдэж байгаа этгээдэд дансаа ашиглуулах эсвэл тэдний өмнөөс банк, санхүүгийн байгууллагад данс нээлгэх, ПИН кодтой банкны карт авах, хувийн код авах, онлайн төлбөрийн системд нэвтрэх эрх авдаг. Ингээд дараа нь тэд гэмт этгээдүүд болон зохион байгуулалттай гэмт бүлэглэлийн гишүүдэд эдгээр мэдээллийг өгөх буюу эрхийг шилжүүлнэ. Мөнгө дамжуулагчид нь ихэнх тохиолдолд өөрсдийн оролцож байгаа үйл ажиллагаа, гэмт хэргийн талаар ямар ч ойлголтгүй байдаг бөгөөд дансаа ашиглуулсны эсвэл "үйлчилгээ" үзүүлсэнийхээ төлөө бага хэмжээний мөнгө авдаг байна.

дамжуулагчдын хувьд гол төлөв ажилгүй, оюутан, тэтгэвэрт гарсан, санхүүгийн хүндрэлтэй хүмүүс байх бөгөөд БИЗ үйлдэгчдэд ашиглагдахаасаа өмнө дансандаа маш бага үлдэгдэлтэй, дансны үйл ажиллагаа нь идэвхитэй бус байх хандлагатай байдаг байна.

6. ЭРСДЭЛИЙГ УДИРДАХ

Банк, санхүүгийн байгууллагууд гүйлгээг шалгаж, баталгаажуулж байж хийх нь БИЗ, луйвраас өөрийн байгууллагыг болон харилцагчийг хамгаалах бололцоог бүрдүүлнэ. Тухайлбал, банк, санхүүгийн байгууллагын ажилтан харилцагчаас гадаад худалдааны төлбөр тооцоо шилжүүлж байгаа данс нь өмнө нь мөнгө шилжүүлж байсан данс мөн эсэх, хэрэв өөрчлөгдсөн бол ямар шалтгаанаар өөрчлөгдөж байгаа талаар асууж тодруулах нь зүйтэй. Мөн шаардлагатай тохиолдолд нэмэлт баримт бичиг, нэхэмжлэх ирүүлсэн имэйл, гэрээг авч шалгах, эсвэл хэрэв харилцагч банк, санхүүгийн байгууллагад имэйлээр гүйлгээний заавар, хүсэлт ирүүлсэн бол харилцагчтай /эсвэл харилцагч байгууллагын өөр эрх бүхий удирдлага, ажилтантай/ утсаар, чатаар, эсвэл бүртгэлтэй өөр имэйл хаягаар /хүсэлт ирүүлсэн имэйл хаягнаас өөр төрлийн холбоо барих хэрэгслээр/ холбогдож гүйлгээг баталгаажуулж болно.

БИЗ амжилттай болох эсэх нь гэмт этгээдүүд харилцагч болон банк, санхүүгийн байгууллагуудыг хууль ёсны мэт харагдах боловч зөвшөөрөлгүй, хууль бус гүйлгээ хийлгүүлэхийн тулд хэр сайн хуурч, ятгаж, итгүүлж чадах эсэхээс хамаардаг. Иймд харилцагч, банк, санхүүгийн байгууллагын ажилтнууд аль аль нь энэ талаар ойлголттой, мэдлэгтэй байх аваас энэ төрлийн залиланд өртөхөөс урьдчилан сэргийлж, хөрөнгө, мөнгийг залилагч этгээдүүд рүү шилжүүлж хохирохоос наана арга хэмжээ авах боломжтой.

Ийм гүйлгээг нэгэнт хийсэн бол ихэнх тохиолдолд буцааж авах боломж маш бага байдаг тул банк, санхүүгийн байгууллагууд болон тэдний харилцагчид гүйлгээг цуцлах, мөнгөө буцааж авах боломжгүй байдаг. Ийм учраас гүйлгээ хийхээс өмнө хуурамч гүйлгээ хийгдэх гэж байгааг олж тогтоох нь зөвшөөрөлгүй, хуурамч гүйлгээ хийгдэх, улмаар хөрөнгө мөнгө, цаг хугацаагаа алдахаас урьдчилан сэргийлэх, энэ төрлийн залилан, луйврыг багасгахад чухал үүрэг гүйцэтгэнэ.

7. ХАРИУ АРГА ХЭМЖЭЭ АВАХ

Эгмонт бүлгийн СМА-уудын зарим гишүүд санхүүгийн байгууллагууд болон хууль сахиулах байгууллагуудтай хамтран БИЗ-тай холбоотой санхүүгийн залилангийн сэжигтэй гүйлгээний мэдээллийг цаг алдалгүй шилжүүлж шалгуулах замаар хохирогчдын хөрөнгө, мөнгийг буцаан олж авахад тусалдаг практик бий. Хохирогч, банк, санхүүгийн байгууллага болон хууль сахиулах байгууллагууд аль болох түргэн шуурхай арга хэмжээ авах нь хохирогчийн хөрөнгө, мөнгийг амжилттай буцаан олж авахад чухал үүрэг гүйцэтгэдэг. Ийм төрлийн залилангийн хувьд алдагдсан хөрөнгө, мөнгийг буцааж олж авах магадлал 24 цаг өнгөрсний дараа мэдэгдэхүйц буурдаг гэж үздэг байна.

БИЗ-ийн хэргийг мөрдөн шалгах, БИЗ-ийн улмаас мөнгөө алдсан хохирогчдын хөрөнгө, мөнгийг буцааж авахад туслах зорилгоор банк, санхүүгийн байгууллагуудад дараах арга хэмжээ авахыг зөвлөж байна.[8] Үүнд:

I. Хууль сахиулах байгууллага болон бусад эрх бүхий байгууллагад яаралтай хандах

а) *Гэмт хэргийн талаар мэдээлэх:* Хохирогч, банк, санхүүгийн байгууллагууд, хууль сахиулах, зохицуулагч байгууллагууд, СМА болон гадаадын СМА-ууд шилжүүлсэн хөрөнгө, мөнгийг буцааж авахын тулд түргэн шуурхай хамтран ажиллах шаардлагатай байдаг. Үүний тулд хохирогч болон хохирогчийн банк, санхүүгийн байгууллага БИЗ, болсон үйл явдлын талаар хууль сахиулах байгууллага болон СМА-нд нэн даруй мэдээлэх нь зүйтэй.

Залилан, луйвар хийх оролдлогын талаарх мэдээлэл нь хууль бус ажиллагаа, гэмт хэргийн сүлжээг шалгахад эрх бүхий байгууллагуудад чухал мэдээлэл болох тул банк, санхүүгийн байгууллагууд зөвхөн амжилттай хийгдсэн БИЗ-ийн гүйлгээнүүдийг мэдээлэхээс гадна энэ төрлийн залилан, луйвар хийх гүйлгээний оролдлогын талаар бас мэдээлж байх нь чухал болохыг анхаарна уу.

б) *Хүлээн авагч банк, санхүүгийн байгууллагад мэдэгдэх:* Хохирогчийн данс байршдаг банк, санхүүгийн байгууллага нь залилан байж болзошгүй сэжигтэй гүйлгээ хийгдсэн талаар шилжүүлгийн гүйлгээг хүлээн авагч банк, санхүүгийн байгууллагатай нэн даруй холбоо барьж мэдэгдэх шаардлагатай.

в) *Хүлээн авсан сэжигтэй шилжүүлгийн гүйлгээг мэдээлэх:* Шилжүүлгийн гүйлгээ хүлээн авч байгаа банк, санхүүгийн байгууллага нь шилжиж орж ирсэн хөрөнгө, мөнгөний эх үүсвэр нь хууль ёсны эсэхэд эргэлзэж байгаа эсвэл хууль бус, гэмт хэргийн замаар олсон хөрөнгө, мөнгө шилжиж орж ирсэн байж болзошгүй гэж сэжиглэж болно. Энэ тохиолдолд банк, санхүүгийн байгууллага уг сэжигтэй гүйлгээний талаар СМА болон хууль сахиулах байгууллагад тэр даруй мэдээлэх хэрэгтэй. СМА-д мэдээлэхдээ Сэжигтэй гүйлгээний тайлангаар хууль, журамд заасан маягтын дагуу нэн даруй мэдээлнэ.

[8] Арга хэмжээ бүрийг заавал дэс дараалсан дагуу хийх албагүй болохыг анхаарна уу. Цаг тухайд нь хариу арга хэмжээ авч, хууль сахиулах байгууллага, СМА зэрэг эрх бүхий байгууллагуудтай хамтран ажиллах нь БИЗ-ийн улмаас алдсан хөрөнгийг буцаан авахад чухал үүрэг гүйцэтгэдэг.

Хэрэв шилжүүлгийн гүйлгээ сүүлийн 72 цагийн дотор хийгдсэн бол гомдол гаргагч хүн, хуулийн этгээд эсвэл банк, санхүүгийн байгууллага хууль сахиулах байгууллага юмуу СМА-нд мэдээлэхдээ “яаралтай” гэдгийг ойлгуулах буюу утсаар мэдэгдэж хэлэх гэх мэтээр аль болох цаг алдалгүй, шаардлагатай арга хэмжээг авах нь зүйтэй.

II. Хөрөнгө, мөнгөний хөдөлгөөнийг зогсоох

а) *Сэжигтэй гүйлгээг хийхгүй байх:* Шилжүүлгийн гүйлгээ хүлээн авагч банк, санхүүгийн байгууллага хэрэв харилцагчийнх нь дансанд хуурамч, залилан луйвартай холбоотой байж болзошгүй гэх мэдээлэл бүхий гүйлгээ хүлээн авсан бол (тухайлбал, СВИФТ-ээр гүйлгээг эргүүлэн татах тухай мессеж ирсэн гэх мэт) тухайн гүйлгээг хийхгүй байх нь зүйтэй. Энэ тохиолдолд хүлээн авсан гүйлгээг шалгаж баталгаажуулах зорилгоор өөрийн дотоод журам, зааврын дагуу шилжүүлэгч банк, санхүүгийн байгууллагатай яаралтай холбогдох, хууль сахиулах байгууллага, СМА зэрэг эрх бүхий байгууллагатай холбогдох хэрэгтэй.

III. Хөрөнгө, мөнгийг битүүмжлэх / буцаан авах

а) *Хөрөнгө, мөнгөний байршлыг эрх бүхий байгууллагуудад мэдээлэх*: Алдсан хөрөнгө, мөнгийг буцааж олж авах магадлалыг нэмэгдүүлэхийн тулд банк, санхүүгийн байгууллага нь хууль сахиулах байгууллагууд болон СМА-нд шаардлагатай бүх мэдээллийг өгч, хамтран ажиллах шаардлагатай. Банк, санхүүгийн байгууллага нь хэрэв гүйлгээ хийгдээгүй, мөнгө нь дансандаа байршиж байгаа бол гүйлгээ хийхээс өмнө энэ талаар СМА болон хууль сахиулах байгууллагад мэдэгдэх, хэрэв гүйлгээ аль хэдийн хийгдсэн бол хөрөнгө, мөнгө хаана явж байгааг, болон эцсийн хүлээн авагчийн байршил, мэдээллийг тодорхой мэдэгдэх нь зүйтэй.

б) *Гүйлгээг түдгэлзүүлэх:* Банк, санхүүгийн байгууллага нь СМА болон эрх бүхий байгууллагаас гаргасан гүйлгээг түдгэлзүүлэх, царцаах шийдвэрийг хууль, журамд заасны дагуу хэрэгжүүлж, хамтран ажиллах шаардлагатай.

8. СЭЖИГТЭЙ ГҮЙЛГЭЭНИЙ ТАЙЛАНГААР МЭДЭЭЛЭХЭД АНХААРАХ ЗҮЙЛ

Банк, санхүүгийн байгууллага нь БИЗ-тай холбоотой сэжигтэй гүйлгээ[9]-ний талаар СГТ-аар мэдээлэхдээ аль болох бүх холбогдолтой бөгөөд дэлгэрэнгүй мэдээллийг тайлбар хэсэгт бичиж мэдээлвэл зохино. Ялангуяа, дараах мэдээллүүдийг СГТ-аар мэдээлэхийг зөвлөж байна. Үүнд:

Шилжүүлгийн гүйлгээний мэдээлэл:

- Сэжигтэй гүйлгээний дүн, хийгдсэн огноо;
- Шилжүүлэгчийн талаарх дэлгэрэнгүй мэдээлэл, дансны дугаар, шилжүүлэгч банк, санхүүгийн байгууллагын мэдээлэл;
- Хүлээн авагчийн талаарх дэлгэрэнгүй мэдээлэл, дансны дугаар, хүлээн авагч банк, санхүүгийн байгууллагын мэдээлэл;
- Корреспондент болон бусад дамжуулагч банкны талаарх дэлгэрэнгүй мэдээлэл.

Залилан үйлдэгдсэн / үйлдэгдэж байгаа схемийн талаарх мэдээлэл:

- Холбогдох имэйл хаягууд, имэйлийн чухал мэдээллүүд агуулагдаж байгаа толгой хэсэг буюу илгээгч, хүлээн авагч, гарчиг хэсгийн мэдээллүүд, интернет протокол буюу IP хаяг зэрэг мэдээллийг цаг хугацааны тэмдэглэгээтэй нь;
- Сэжигтэй гэж үзэж байгаа имэйл харилцааны талаарх мэдээллийг цаг хугацааны тэмдэглэгээтэй нь тус тус мэдээлэхийг зорих нь зүйтэй.

[9] Сэжигтэй гүйлгээ гэдэгт хийгдсэн сэжигтэй гүйлгээ болон хийхийг завдсан сэжигтэй гүйлгээний оролдлогыг аль алиныг хамруулж ойлгоно.

9. ХАВСРАЛТ – КЭЙС ЖИШЭЭ

КЭЙС 1.

Шинж тэмдэг:

- Залилан, луйврын үйл ажиллагаа
- Хуурамч баримт бичиг ашигласан
- Халхавч хүн / компани ашигласан
- Сэжигтэй гүйлгээ хийсэн / хөрөнгө, мөнгийг богино хугацаанд шилжүүлсэн

2016 оны 1 дүгээр сард СМА нь"Б" улсад үнэртэй ус, гоо сайхны бүтээгдэхүүний худалдаа эрхэлдэг А компанитай холбоотой сэжигтэй гүйлгээний мэдээлэл хүлээн авсан. А компани нь 2015 оны 11 дүгээр сарын дунд үеэс 2015 оны 12 дугаар сарын эцэс хүртэл 7 удаагийн шилжүүлгээр нийт 5 сая еврогийн дүнтэй гадаад гуйвуулгын гүйлгээг "Д" улс дахь банкны данс руу шилжүүлсэн байна.

А компанийн 2016 оны 1 дүгээр сард гаргасан гомдолд дурдсанаар А компанид бараа бүтээгдэхүүн нийлүүлдэг компанийг төлөөлж нэгэн үл таних хүн цаашид бараа бүтээгдэхүүний нэхэмжлэхийн төлбөрийг гэрээнд зааснаас өөр банкны данс буюу Д улс дахь банкны данс руу шилжүүлж байх талаар мэдэгджээ. А компанийн дотоод журмын дагуу ийм тохиолдолд нийлүүлэгч компанийн өөр ажилтантай холбоо барьж баталгаажуулах ёстой байдаг бөгөөд энэ дагуу холбоо барихад нийлүүлэгч компанийн Санхүү хариуцсан гүйцэтгэх захирлын мэдээлэл (жинхэнэ нэр болон хуурамч утасны дугаар)-ийг өгсөн байна. А компанийн жинхэнэ нийлүүлэгч компаниас сүүлд ирүүлсэн нэхэмжлэлүүд дээр өмнөх хэд хэдэн худалдан авалтын төлбөр төлөгдөөгүй үлдэгдэлтэй байснаар энэ залилан илэрчээ. Залилагч этгээд А компанийн ажилтны дүр эсгэн, нийлүүлэгч компани руу имэйл бичиж, төлбөр шилжүүлэхэд асуудал гарсан тул шилжүүлээгүй нэхэмжлэхийн төлбөрүүдийг хугацаа хожимдож төлөх болсон талаар урьдчилан мэдэгдсэн байсан тул нийлүүлэгч нь А компанитай энэ талаар ярилцалгүй, зөвхөн дараагийн нэхэмжлэхүүд дээр үлдэгдлийг оруулан илгээж байсан байна.

"Б" улсын СМА нь "Д" улсад А компаниас шилжүүлсэн мөнгийг хүлээн авсан банкны данс эзэмшигч / төлөөний хүн / эцсийн өмчлөгчийн дэлгэрэнгүй мэдээлэл, дансны үлдэгдэл, шилжүүлсэн мөнгийг цааш яаж хөдөлгөсөн зэргийг тодруулахаар "Д" улсын СМА-нд яаралтай хүсэлт илгээсэн байна.

Дараагийн өдөр нь "Д" улсын СМА-наас хариу мэдээлэл ирүүлсэн бөгөөд мөнгө хүлээн авсан банкны данстай холбоотой сэжигтэй гүйлгээний тайлан мэдээлэгдэж байсан талаарх мэдээллийг өгсөн. Энэ банкны дансыг "Д" улсад электрон барааны худалдаа эрхэлдэг Ц компанийн нэр дээр саяхан нээлгэсэн бөгөөд уг компанийн гүйцэтгэх захирал байсан хүн болон иргэн Х нар банканд ирж нээлгэсэн байна. Данс нээлгэснээс хэдэн долоо хоногийн дараа компанийн өмчлөлд өөрчлөлт орж, иргэн Х тус компанийн гүйцэтгэх захирал бөгөөд хувьцаа эзэмшигч нь болжээ.

"Б" улсын банк "Д" улсын банк руу гадаад шилжүүлгийн 7 гүйлгээг цуцлах хүсэлт хүргүүлсэн боловч мөнгө хүлээн авсан компани нь А компаниас хүлээн авсан мөнгийг аль хэдийн Зүүн Азийн хоёр улсын хэд хэдэн банкны данс руу шилжүүлсэн нь тогтоогдсон байна.

КЭЙС 2.

Шинж тэмдэг:

- Компанийн удирдах албан тушаалтан төлбөр хүлээн авах дансны мэдээллийг гэнэт өөрчилсөн
- Төлбөр төлөх дансны мэдээллийг өөрчлөх болсон шалтгааныг дурдаагүй
- Албан бус имэйл хаяг эсвэл хуурамч баримт бичиг ашигласан
- Хувь хүн өмнө нь холбоогүй байсан байгууллагаас өндөр дүнтэй шилжүүлэг хүлээн авсан
- Хүлээн авсан мөнгийг тэр дор нь гадаад улс руу шилжүүлсэн
- Богино хугацааны дотор өөр өөр байршил дахь хэд хэдэн улс руу шилжүүлгийн гүйлгээ хийсэн /мөн өндөр эрсдэлтэй бүс нутагт харьяалагдах улс руу мөнгө шилжүүлсэн/

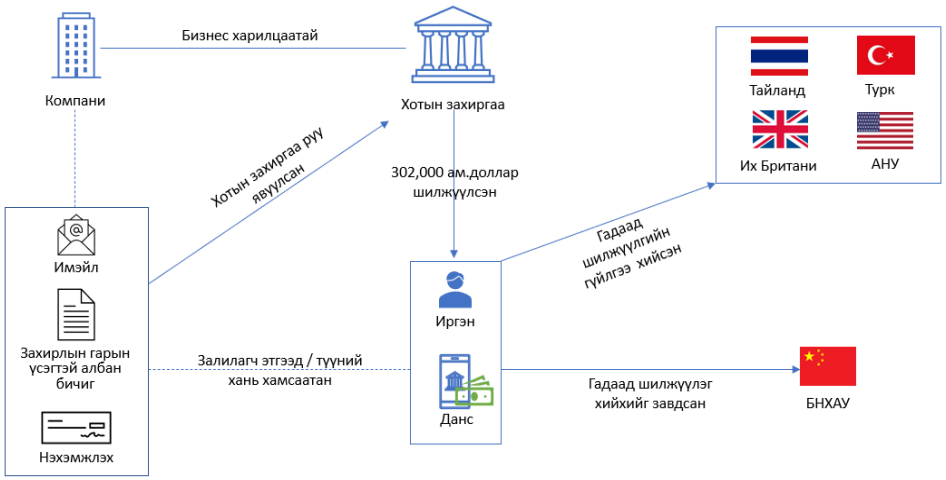
А улсын Хотын захиргаа бизнес имэйл залиланд өртөж, 302,000 орчим ам.доллар залилуулсан байна.

Тус Хотын захиргаа нь хамтран ажилладаг компаниасаа төлбөр шилжүүлэх банкны данс өөрчлөгдсөн талаар мэдэгдсэн имэйл хүлээн авсан. Имэйлд төлбөр хүлээн авах банк, дансны шинэ мэдээллийг хүргүүлж байгаа тухай компанийн гүйцэтгэх захирлын гарын үсэг зурсан албан бичиг, компанийн нэр, лого бүхий төлбөрийн нэхэмжлэхийг хавсаргасан байв.

Энэ залилан нь дээрх компанийн зээлийн хяналтын нэгжээс Хотын захиргааны төлөх ёстой төлбөрийн үлдэгдэл 302,000 ам.доллар байгааг нэхэмжилж, Хотын захиргаанаас энэ төлбөрийг аль хэдийн төлсөн талаар мэдэгдсэнээр илэрсэн байна. Улмаар Хотын захиргаанд өмнө ирүүлсэн нэхэмжлэх, имэйл, албан бичгийг шалгахад компанийн ашигладаг имэйл хаягнаас өөр имэйл хаягнаас хуурамч хэвлэмэл хуудсан дээр бичсэн албан бичиг ирүүлсэн бөгөөд компанийн гүйцэтгэх захирлын гарын үсгийг дууриалган зурсан болохыг тогтоожээ.

Хотын захиргаанаас ийнхүү хуурамч имэйл, баримт бичгийн дагуу шилжүүлсэн мөнгийг А улсын нэгэн иргэн дансандаа хүлээн авч, тэр дор нь Тайланд, Турк, Их Британи, АНУ дахь компаниуд руу шилжүүлсэн байна. Мөн БНХАУ руу шилжүүлэхийг завджээ.

Хотын захиргаа БИЗ-ийн улмаас алдсан мөнгөө буцаан олж авч чадаагүй байна.



КЭЙС 3.

Шинж тэмдэг:

- Байгууллагын удирдах албан тушаалтнаас яаралтай мөнгө шилжүүлэх заавар ирүүлсэн
- Мөнгө шилжүүлэх учир шалтгааныг дурдаагүй
- Удирдах албан тушаалтан эзгүй үедээ имэйлээр мөнгө шилжүүлэх заавар өгсөн
- Төлбөр тооцоо, гүйлгээ хийгдэх ердийн горимыг мөрдөөгүй
- Толгой хэсэгт харагдах имэйл хаяг нь буцах имэйл хаягнаас өөр байсан

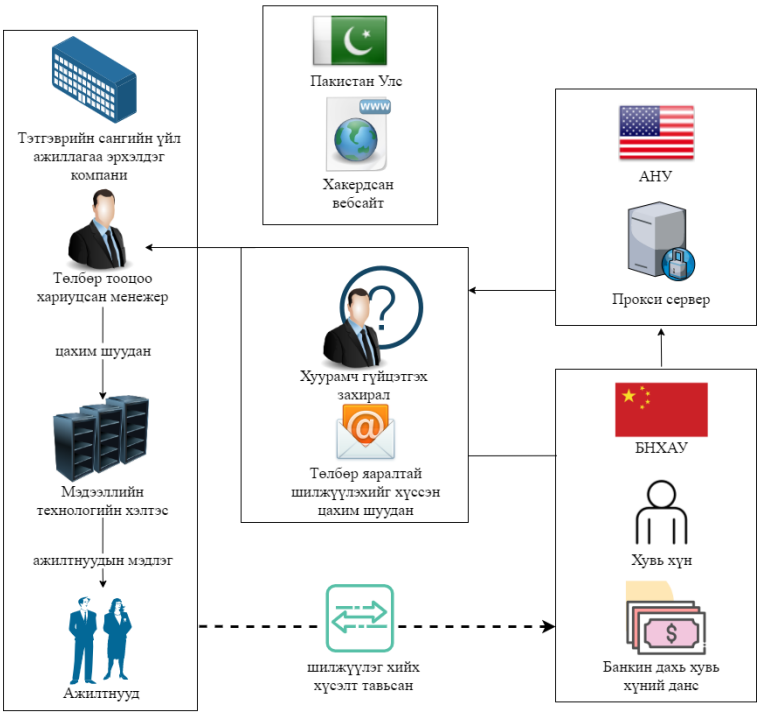
А улсад тэтгэврийн сангийн үйл ажиллагаа эрхэлдэг компани БИЗ хийх оролдлогод өртсөн байна. Тус компанийн төлбөр тооцоо хариуцсан менежерт компанийн гүйцэтгэх захирлаас БНХАУ-ын банкин дахь хувь хүний данс руу 225,000 ам.долларыг яаралтай шилжүүл гэсэн утгатай хэд хэдэн имэйл иржээ.

Менежер эдгээр имэйлийг хуурамч ба залилан, луйвартай холбоотой байж болзошгүй гэж сэжиглэн, компанийн Эрсдэл хариуцсан хэлтэс болон Мэдээллийн технологийн хэлтэст шалгуулахаар хандсан байна. Мэдээллийн технологийн хэлтэс шалгаад дээрх имэйлүүд нь гүйцэтгэх захирлын имэйл хаягнаас ирсэн мэт харагдахаар далдалсан, хуурамч имэйл хаягнаас ирүүлсэн болохыг тогтоожээ. Мөн и-мэйл хаягийг үүсгэсэн вэбсайт нь Пакистанаас хакердсан вэбсайт болохыг олж тогтоосон байна. Дээрх имэйлүүдийг АНУ дахь этгээдээр дамжуулан БНХАУ-аас илгээсэн байв.

Залилан мэхлэгчид имэйл илгээх үед гүйцэтгэх захирал эзгүй байсныг мэдэж байсан бөгөөд компанийн системд хууль бусаар нэвтэрсэн байж болзошгүй гэж үзсэн байна.

Компанийн менежер, ажилтнууд гүйцэтгэх захирлаас нь ирүүлсэн имэйлүүд хуурамч байсныг олж тогтоосон тул ямар нэг шилжүүлэг хийж хохироогүй байна. Харин энэ асуудалтай холбогдуулан залилан мэхлэх оролдлого, БИЗ эсвэл цахим халдлага хийх аливаа оролдлогоос цаашид өөрийн компанийг хамгаалах, урьдчилан сэргийлэх зорилгоор дараах арга хэмжээнүүдийг авсан байна. Үүнд:

- Хуурамч имэйл ирүүлсэн хаягийг блоклосон.
- Залилан мэхлэгчийн ашигласан IP хаягийг блоклосон.
- Аливаа вирус, хортой програмыг тодорхойлохын тулд компанийн бүх системд скан хийсэн.
- Толгой дээр харуулсан имэйл хаягнаас өөр имэйл хаягнаас имэйл ирэхэд блоклох тохиргоог компанийн системд хийж өгсөн.
- Компанийн ажилтнуудад БИЗ, цахим халдлага хийх оролдлогын талаар мэдээлэл, мэдлэг олгох сургалтын цогц хөтөлбөр хэрэгжүүлсэн.
- Дотоод журамд зааснаас өөрөөр төлбөр тооцоо хийхгүй байх, хэрэв өөр бөгөөд сэжиг бүхий хүсэлт, заавар ирсэн тохиолдолд энэ талаар нэн даруй мэдэгдэх ёстой талаар бүх ажилтнуудад мэдэгдсэн.
- Сэжиг бүхий имэйлийн талаар мэдээлсэн ажилтнуудыг урамшуулах болсон талаар танилцуулсан байна.


Тэтгэврийн сангийн үйл ажиллагаа эрхэлдэг компани
Төлбөр тооцоо хариуцсан менежер
цахим шуудан
Мэдээллийн технологийн хэлтэс
ажилтнуудын мэдлэг
Ажилтнууд
Пакистан Улс
Хакердсан вебсайт
Хуурамч гүйцэтгэх захирал
Төлбөр яаралтай шилжүүлэхийг хүссэн цахим шуудан
шилжүүлэг хийх хүсэлт тавьсан
АНУ
Прокси сервер
БНХАУ
Хувь хүн
Банкин дахь хувь хүний данс

КЭЙС 4.

Шинж тэмдэг:

- Санхүүгийн гүйлгээ нь харилцагч, үйлчлүүлэгчийн профайлтай тохирохгүй байв
- Хохирогчид маш үнэтэй бэлэг санал болгосон
- Өндөр дүнтэй татварын төлбөрийг хувь хүний данс руу шилжүүлүүлсэн

Хайр дурлалын залилан, луйварт өртөж хохирдог хүмүүс ихэвчлэн ганц бие эсвэл ганцаардмал хүмүүс байдаг бөгөөд тэд Facebook, Whatsapp, онлайн болзооны вэбсайт гэх мэт онлайн болон сошиал медиа платформ ашиглан залилагч этгээдтэй танилцаж, харилцаа холбоо тогтоож эхэлдэг байна. Залилагч этгээд хохирогчдыг "илгээсэн бэлэгний тодорхой хувийг шилжүүлнэ үү", "эмнэлгийн яаралтай тусламжийн төлбөр хэрэгтэй боллоо" гэх юмуу эсвэл өөр бусад шалтаг, шалтгаан тоочиж тодорхой хэмжээний мөнгийг өөр лүү нь эсвэл "мөнгө дамжуулагч" буюу залилагч этгээдийн хяналтад байх данс руу шилжүүлэхийг ятгадаг.

Энэ төрлийн залилангийн жишээг дурдвал: "Царайлаг, хөгжилтэй, баян залуу" Майк (залилагч этгээд) фэйсбүүкээр 40 орчим насны ганц бие эмэгтэй А-д найзын хүсэлт илгээн танилцжээ. Зохиомол нэр, хуурамч зураг бүхий Майк хатагтай А-ийн итгэлийг олж авахын тулд фэйсбүүкээр байнга харилцаж байв. Майк хатагтай А-г өөрт нь их таалагдаж байгаа ба түүнд үнэхээр татагдаж байгаа гэж итгүүлж, А-тай үерхэж, урт хугацааны харилцаа үүсгэх хүсэлтэй байгаагаа илэрхийлжээ. Ийм төрлийн залилан, луйварт өртөгсдийн нэгэн адил хатагтай А өөрийгөө урхинд орсон гэж сэжиглэлгүй, түүнд итгэсэн байна.

Майк хатагтай А-д хайр сэтгэл, үнэнч тууштай байдлаа батлахын тулд түүнд маш үнэтэй бэлэг илгээсэн гэж хэлжээ. Хожим нь хохирогч руу шуудангийн компанийн ажилтан гэх хүн ярьж, түүнд бэлэг /илгээмж/ ирсэн бөгөөд илгээмжийг гааль дээр хурааж авсан, гаалиас авахад үнийн дүнгээс хамаарч гаалийн татвар 10,000 ам.доллар (ойролцоогоор 9,400 евро) төлөх ёстой гэж хэлсэн байна. Мөн хатагтай А-д банкны дансны дугаар өгсөн бөгөөд гаалийн татварыг энэ данс руу шилжүүлэх ёстой гэж хэлжээ.

Хатагтай А ямар нэг сэжиг авалгүй хадгаламжийн данснаасаа 10,000 ам.доллар шилжүүлсэн байна. Маргааш нь тэрээр шуудангийн компани руу залгаж, гаалийн татвар төлсөн гэдгээ мэдэгдэж, илгээмжийг хурдан түүнд хүргэхийг хүсэв. Шуудангийн компани түүн рүү хэзээ ч утасдаагүй, түүний нэр дээр ямар ч бэлэг, илгээмж ирээгүй, мөн илгээмж хүлээн авагч татвар төлөх ямар нэг журам байхгүй талаар хэлж, хатагтай А-г цагдаагийн байгууллагад хандахыг зөвлөжээ.

Цагдаагийн байгууллагаас шалгалт явуулахад хатагтай А-ийн шилжүүлсэн мөнгө нэгэн оюутны хадгаламжийн данс руу орсон бөгөөд уг оюутан нь гадаад иргэнээс бага хэмжээний мөнгө авч, өөрийн данс, интернет банк, АТМ картаа ашиглуулж байсан нь тогтоогдсон байна. Оюутан түүний дансыг хууль бус үйл ажиллагааны зорилгоор ашиглаж байсныг мэдэж байв. Мөрдөн шалгах ажиллагааны явцад Майк болон түүний хамсаатан нь утасны дугаарыг хуурамчаар харуулах технологи ашиглан хатагтай А руу жинхэнэ шуудангийн компанийн утаснаас залгаж байгаа мэт ярьж, залилан мэхэлсэн байна.

КЭЙС 5.

Шинж тэмдэг:

- Харилцагчийн хэвийн бус, сэжигтэй үйлдэл
- Шилжүүлгийн дүн маш өндөр
- Гүйлгээ нь харилцагчийн хийдэг ердийн гүйлгээнээс өөр, ажил, бизнесийн үйл ажиллагаатай нь нийцээгүй

Гэмт этгээдүүд 8 дугаар сарын 11-ний өдөр Л улсын нэгэн компанитай холбоо барьжээ. Тэд компанийн ажилтныг БНХАУ-ын банкны данс руу 10,764,000.84 евро (ойролцоогоор 11.5 сая ам.доллар) -ийн шилжүүлэг хийхийг ятгажээ. Компанийн данс байрших банк уг гүйлгээг хийлгүй зогсоосон байна.

Дараа нь гэмт этгээдүүд Ф улс дахь банкны дансаа өгч, дахин мөнгө шилжүүлүүлэхийг оролджээ. Банк өмнөхтэй адил гүйлгээг нь хийхээс татгалзсан байна.

Компанийн ажилтан тэр өдрөө дахин банкинд хандаж Ф улс дахь банкны данс руу 980,000 евро (ойролцоогоор 1 сая ам.доллар) шилжүүлэх хүсэлт тавьсан байна. Банк шилжүүлэг хийхээс мөн татгалзав.

Эдгээр гүйлгээнүүд нь хийгдээгүй буюу зөвхөн гүйлгээ хийх оролдлого байсан хэдий ч банк 8 дугаар сарын 18-ны өдөр Л улсын СМА-нд Сэжигтэй гүйлгээний тайлангаар мэдээлэв. Л улсын СМА нь мэдээллийг Ф улсын СМА руу тэр даруй шилжүүлсэн бөгөөд Ф улсын СМА 8 дугаар сарын 21-ний өдөр хариу ирүүлэв. Хариугаар данс эзэмшигчийн талаарх дэлгэрэнгүй мэдээллийг ирүүлээд, залилан, луйвар хийх оролдлогын талаар холбогдох банканд мэдэгдсэн ба банк уг харилцагчийн дансанд хяналт тавихаар болсон талаар мэдээлжээ.

9 дүгээр сарын 8-ны өдөр Ф улсын СМА нь дээрх дансанд Л улсын өөр нэг компаниас 2 сая евро (ойролцоогоор 2.1 сая ам.доллар) шилжүүлсэн тухай Л улсын СМА-нд мэдэгдэж, энэ гүйлгээ нь залилан, луйвартай холбоотой эсэхийг лавласан байна. Ф улсын СМА нь уг гүйлгээ хууль ёсны эсэхийг шалгаж баталгаажуултал дансны гүйлгээг түдгэлзүүлжээ.

Л улсын СМА нь хууль сахиулах байгууллагатай хамтран мөнгө шилжүүлсэн компанитай холбогдож, холбогдох баримт бичиг, гүйлгээг шалгасан байна. Ингээд 9 дүгээр сарын 9-ний өдөр Л улсын СМА нь Ф улсын СМА-нд 2 сая еврогийн шилжүүлэг залилан, луйварт өртсөн, хууль бус гүйлгээ болохыг мэдэгдсэний үндсэн дээр Ф улс мөнгийг хохирогчийн данс руу буцаан шилжүүлсэн байна.

КЭЙС 6.

СГТ-ийн сэжиглэх үндэслэл:

- Харилцагчийн залилан, луйварт өртсөн гүйлгээ

Банкны харилцагч Т нь дараах утгатай мэдээлэл бүхий и-мэйлийг logisticsexpress00@gmail.com хаягнаас хүлээн авсан байна:

“*Сайн байна уу хадагтай*

Зөвшөөрлийн явцад дотор нь асар их хэмжээний мөнгө байдаг нь тогтоогджээ.

Багц дотор 48,000 доллар (136,913,766 монгол төгрөг) байгаа.

Мөнгө угаах болон терроризмыг санхүүжүүлэхтэй тэмцэх арга хэмжээний талаар Санхүүгийн үйл ажиллагааны ажлын хэсгийн (FATF) өгсөн зөвлөмжийг зохих ёсоор биелүүлээгүйн улмаас Монгол Улс FATF-ийн саарал жагсаалтад Ирак, Зимбабве улсын хамт орсон байна. 2019 оны 10-р сарын 4-ний өдөр ФАТФ нь 1989 онд байгуулагдсан засгийн газар хоорондын байгууллага бөгөөд мөнгө угаах, терроризмыг санхүүжүүлэх болон бусад олон улсын санхүүгийн системийн бүрэн бүтэн байдалд заналхийлэхтэй тэмцэх зорилгоор байгуулагдсан.

2017 онд харилцан үнэлгээний тайлангаа (MER) боловсруулж дууссанаас хойш Монгол улс техникийн нийцэл, үр ашгийг дээшлүүлэх чиглэлээр MER-ийн зөвлөсөн хэд хэдэн арга хэмжээний талаар ахиц дэвшил гаргасан. Монгол Улс 40 техникийн шаардлага хангаснаас 35-ыг нь хийж гүйцэтгэснээс 11-ээс долоог нь хийжээ.

Монгол Улсын техникийн нийцлийн үнэлгээний хүсэлтийг үнэлэх, бэлтгэл ажлыг хангах чиглэлээр ажиллаж байсан шинжээчид Монгол Улс бүх гадаад гүйлгээ, хөрөнгө оруулалтыг эрсдэлд оруулж, эдийн засгийг удаашруулж, цаашид тодорхойгүй байдалд хүргэж байна.

Монгол Улс 2014 онд мөнгө угаахтай холбогдсон арга хэмжээ авсны дараа саарал жагсаалтаас гарч чадсан удаатай. Монгол Улс 2017 оноос хойш FATF-ийн стандартад нийцсэн техникийн сул талуудыг арилгах чиглэлээр ажиллаж ирсэн.

Монгол Улс Саарал жагсаалтад орсны дараа Монголбанк (Төв банк) болон Монгол Улсын засгийн газар хамтран FATF-ийн саарал жагсаалтаас 2020 оны долдугаар сард батлагдсан MER-д тогтоосон техникийн нийцлийн дутагдлыг арилгах чиглэлээр ахиц дэвшил гаргах замаар гарахыг зорьж байна. 2017 он.

Мөнгийг хуульчлахад 2550 доллар (7,273,543) долларын төлбөр шаардлагатай.

Тун удахгүй төлбөрөө хийхийн тулд бидэнд хариу бичнэ үү”

Иргэн Т энэ и-мэйлийн дагуу И Улсын банкны данс руу нийт 10,412 ам.долларыг 3 удаагийн шилжүүлгээр шилжүүлж, цахим залиланд өртсөн байна.

Банк эдгээр гүйлгээг Сэжигтэй гүйлгээний тайлангаар СМА-нд мэдээлсэн ба СМА дүн шинжилгээ хийж, цагдаагийн байгууллагад шилжүүлсэн.

КЭЙС 7.

СГТ-ийн сэжиглэх үндэслэл:

- Харилцагчийн луйварт өртсөн гүйлгээ

Банкны харилцагч, иргэн М рүү эмэгтэй хүний хаягнаас чат бичиж "*Манай ээж монгол хүн байсан, аав маань америк хүн байсан. Манай аав, ээж, бид 3 намайг 8 настай байхад осолд орж, би ганцаараа амьд үлдсэн"* гээд нэлээд удаан хугацаанд чатаар харилцаж байсан байна. Цаашлаад "*Би Монголд очмоор байна, би тан руу өөрийн ачаагаа явуулахыг хүсэж байна, энэ ачаан дотор манай гэр бүлийн эрдэнэ байгаа, энэ ачаа ямарч асуудалгүй тан дээр очино, би араас нь очиж ачаагаа авна*" гэж бичсэн бөгөөд иргэн М итгэн, өөрийн гэрийн хаягийг өгчээ. Маргааш нь "*би ачаагаа явуулчихлаа, энэ ачааг авч явах дипломатч тан руу холбогдоно"* гэсэн ба удалгүй дипломатч гэх хүн залгаад "*ачааг чинь авчихлаа, та гаалийн төлбөр төлөх ёстой*" гэж хэлсэн байна. Иргэн М "*энэ төлбөрийг ачаа илгээгч төлөх байх, би сайн мэдэхгүй*" гэхэд "*үүнийг хүлээн авагч төлдөг юмаа, энийг та төлөх ёстой*" гэхээр нь иргэн М илгээгч бүсгүйгээс энэ талаар чатаар асуухад *"та энэ төлбөрийг төлж өгөөч"* гэж. Хариуд нь "*надад мөнгө байхгүй, би төлж чадахгүй*" гэхэд "*наад ачаанд чинь их хэмжээний бэлэн мөнгө байгаа"* гэж хэлэн мөнгөний зурагнууд илгээсэн бөгөөд "*та энэ мөнгийг төлөхгүй бол хоёулаа баригдаж шоронд сууна, харин төлөх юм бол би танд ачаа очсоны дараа мөнгийг чинь нэмж өгнө*" гэж хэлсэн байна.

Ингээд иргэн М тэр төлбөрийг нь төлөөд байж байтал дахин 2 төлбөр нэхсэн ба эдгээр төлбөрийг мөн төлсөн байна. Харин 4 дэх удаагаа төлбөр нэхэх үед нь тэрээр интернетээс судалж үзэхэд өөр шиг нь луйвардуулсан хүмүүс байсныг олж мэдсэн байна.

Иргэн М ийнхүү цахим залиланд өртөж, гаалийн татвар, терроризмын эсрэг бичгийн мөнгө, ачаа тээврийн даатгалын мөнгө гэж нийт 40,270,240 төгрөгийг 3 удаагийн шилжүүлгээр шилжүүлсэн байна.

Банк эдгээр гүйлгээг Сэжигтэй гүйлгээний тайлангаар СМА-нд мэдээлсэн ба СМА дүн шинжилгээ хийж, цагдаагийн байгууллагад шилжүүлсэн.

_____oOo_____