КИБЕР АЮУЛГҮЙ БАЙДАЛД НҮҮРЛЭСЭН ШУУРГЫГ НАМЖААХ УРЛАГ

УДИРТГАЛ

Техник технологид суурилсан энэ цаг үед кибер халдлагын давтамж өдөр бүр нэмэгдэж, улам боловсронгуй болж байгаа бөгөөд үүнтэй холбоотойгоор кибер аюулгүй байдал нь байгууллагууд төдийгүй хувь хүмүүсийн анхаарах зайлшгүй шаардлагатай чухал асуудал болоод байгаа билээ. Тиймээс иргэн та кибер аюулгүй байдлын зөрчилд өртсөн тохиолдолд хэрхэх тухай мэдлэг, ойлголтой байх нэн чухал юм. Учир нь кибер зөрчлөөс үүдэх хор хохирол нь зөвхөн хүний хувийн мэдээлэл, аккаунт алагдагдсанаар зогсохгүй цаашлаад тухайн хүний санхүү, нэр хүнд, бүр амь насанд ч хүрэхүйц сөрөг үр дагавар авчирч болзошгүй юм. Жишээ нь магадгүй халдагч этгээд таны хувийн мэдээллийг ашиглан бусдыг залилан мэхлэх, эсвэл таны хаяг бүртгэлүүдээр нэвтрэн хууль бус үйл ажиллагаа явуулах зэрэг эрсдэлүүд байдаг. Тиймээс энэ удаа кибер зөрчил тохиолдох үед хэрхэн шийдвэрлэх тухай, зөрчилд хариу үзүүлэх арга хэмжээ болон мэргэжлийн байгууллагад хандан тусламж зөвлөгөө авч болох талаарх ойлголтуудыг хүргэж байна.

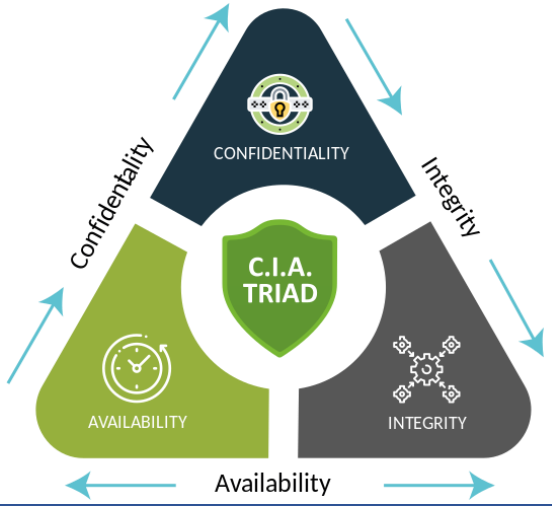
ҮНДСЭН АГУУЛГА

Хамрах хугацаа:	**2024 оны 7-р сарын эхний хагас (#1)**
Хамрах сэдэв:	**Кибер зөрчил, түүнд хариу үзүүлэх болон түүн дэх CERT-ын үүрэг, оролцооны тухай**

📌 **Кибер зөрчил ❗ :**

Мэдээллийн нууцлагдсан, бүрэн бүтэн, хүртээмжтэй байдалд болзошгүй эсвэл бодит сөрөг нөлөө үзүүлж байгаа аливаа үзэгдлийг кибер зөрчил гэнэ. Өөрөөр хэлбэл кибер аюулгүй байдлын аюул заналын тохиолдсон байж болзошгүй эсвэл бодитоор тохиолдож буй байдлыг хэлдэг. Жишээ нь дараах үзэгдэл, үйлдлүүд байж болно. Үүнд:

a. ⚠️ Сүлжээ, систем эсвэл өгөгдөлд зөвшөөрөлгүй нэвтрэх



b. ⚠️ Өгөгдлийг зөвшөөрөлгүй хадгалах, түгээх
c. ⚠️ Техник хангамж эсвэл программ хангамжийг зөвшөөрөлгүй өөрчлөх
d. ⚠️ Сүлжээний орчинд сервисүүд болон системийг тасалдуулах
e. ⚠️ Өгөгдлийг санаатай эсвэл санамсаргүй байдлаар задруулах

Эдгээр үзэгдлүүд нь бидний мэдэх түгээмэл аюул занал, халдлагуудтай холбоотой байж болно. Тухайлбал,

- ⛔Өгөгдөл алдагдах буюу эмзэг нууц мэдээлэлд зөвшөөрөлгүй хандах нь нууцлагдсан байдлыг алдагдуулна.
- ⛔Рансомвэйр халдлага буюу өгөгдлийг шифрлэж, төлбөр төлөхийг шаарддаг хортой программ нь хүртээмжтэй байдлыг алдагдуулна.
- ⛔Фишинг халдлага буюу эмзэг нууц мэдээлэл олж авах гэсэн залилангийн оролдлого нь нууцлагдсан байдлыг алдагдуулна.
- ⛔DoS халдлага буюу их хэмжээний олон тооны хүсэлтийг илгээх замаар үйлчилгээг тасалдуулах нь хүртээмжтэй байдлыг алдагдуулна.

Кибер зөрчлүүд нь олон талын сөрөг нөлөө, хор хохиролыг байгууллага болон хувь хүмүүст учруулдаг бөгөөд хамгийн ноцтой зөрчил нь мэдээллийн нууцлал алдагдах ба энэ нь цаашлаад санхүү, нэр хүнд гэх зэрэгт сөрөг нөлөө үзүүлнэ. Тиймээс кибер зөрчил тохиолдсон үед цаг алдалгүй хурдан хариу арга хэмжээ авах нь хамгаас чухал юм. Учир нь хугацаа өнгөрөх тусам учрах хохирлын хэмжээ нэмэгдсээр байдаг. Дараах хэсэгт кибер зөрчилд хэрхэн хариу үзүүлэх арга хэмжээний тухай хүргэе.

📌 **Кибер зөрчилд хариу үзүүлэх нь ❗ :**

🔥💥Кибер зөрчил тохиолдсон үед хурдан шуурхай хариу арга хэмжээ авч, цааш холбогдох байгууллагууд руу мэдээлэх нь кибер зөрчлийн улмаас учирч болох хохирлыг бууруулахад чухал ач холбогдолтой. Яаралтай, хурдан арга хэмжээ авснаар мэдээлэл алдагдахаас сэргийлж, нууц мэдээллийг хамгаалж, санхүүгийн болон нэр хүндэд үзүүлэх сөрөг нөлөөллийг бууруулж чадна.

⏳🎯Харин зөрчил тохиолдсон үед иргэн та хэрхэн шийдвэрлэх талаар мэдэхгүй байвал танд туслалцаа үзүүлэх чиг үүргийн байгууллага байдаг бөгөөд та өөрт тулгараад буй кибер зөрчлийн талаар чиг үүргийн байгууллага руу мэдэгдэж, хамтран ажилласнаар буюу хамтран зөрчилд хариу үзүүлснээр зөрчлийг шийдвэрлэх, зөрчлийн үндсэн шалтгааныг тогтоох, дахин уг зөрчил тохиолдохоос сэргийлэх арга хэмжээ авах боломжтой байдаг. Ингэснээр кибер зөрчилд үр дүнтэйгээр хариу үзүүлж, учирж болох хохирлыг багасгаад зогсохгүй, мөн уг зөрчил ирээдүйд

дахин тохиолдохоос сэргийлж чадах юм. Уг чиг үүрэг бүхий байгууллага нь кибер зөрчилд хариу үзүүлэх байгууллага буюу олон улсад CERT эсвэл CSIRT гэсэн нэршлээр танигдсан байдаг. Ингээд дараагийн хэсэгт уг чиг үүргийн байгууллагын тухай товч танилцуулъя.

📌 **Кибер зөрчилд хариу үзүүлэхэд CERT-ын үүрэг, оролцооны тухай ❗ :**

CERT (**C**omputer **E**mergency **R**esponse **T**eam) буюу кибер зөрчилд хариу үзүүлэх баг/компьютерын яаралтай тусламжийн баг нь зөрчилд хариу үзүүлэх болон зөрчлийг бууруулахад чухал үүрэгтэй. Анхны CERT нь 1988 онд Пенсильвани мужийн Питтсбург хотын Карнеги Меллон их сургуульд байгуулагдсан. Үүнийг Компьютерын зөрчилд хариу арга хэмжээ авах баг/зохицуулах төв (CERT/CC) гэж нэрлэсэн бөгөөд уг "CERT" нэршил нь Карнеги Меллон Их Сургуулийн бүртгэлтэй ялгах тэмдэг бөгөөд хэрэглээг нь тодорхой удирдамжаар зохицуулдаг. Тиймээс кибер аюулгүй байдлын салбарт кибер зөрчилд хариу үзүүлэх багийг CSIRT (**C**omputer **S**ecurity **I**ncident **R**esponse **T**eam) гэсэн нэршлээр төлөөлүүлдэг.

👩‍💻🙌CERT/CSIRT-ийн чиг үүрэгт байгууллага эсвэл хувь хүн, түүний өгөгдөл, компьютер, сүлжээ, систем, программ хангамж зэрэг мэдээллийн хөрөнгөд заналхийлж буй аюул заналаас урьдчилан сэргийлэх, кибер зөрчлийн болзошгүй тохиолдлыг илрүүлэх, хариу үзүүлэх зэрэг багтдаг. Өөрөөр хэлбэл, CERT/CSIRT нь байгууллага болон хувь хүнд кибер аюулгүй байдлын аюул занал болон зөрчлийн нөлөөллийг багасгаж, кибер аюулгүй байдлын ерөнхий төлөв байдлыг сайжруулахад мэргэжлийн туслалцаа, дэмжлэг үзүүлдэг.

Тэгвэл дээр дурдсан “хамгаалах, илрүүлэх, хариу үзүүлэх” загварын хувьд CERT/CSIRT нь дараах үүрэг, оролцоотой байна.

- 🔐Хамгаалах 🛡️ – Зөрчилд хариу үзүүлэх төлөвлөгөө гаргах, эрсдэлийн үнэлгээ хийх, эмзэг байдлын шалгалт хийх, халдлага илрүүлэх систем ашиглах зэрэг кибер аюулаас урьдчилан сэргийлэх идэвхтэй арга хэмжээг хэрэгжүүлнэ.
- 🔎Илрүүлэх 🚨 – Кибер зөрчил болон зөрчлийн болзошгүй тохиолдол, сэжигтэй үйлдэл, үзэгдлүүдийг илрүүлэх төрөл бүрийн технологи болон бусад эх сурвалжаас ирүүлсэн мэдээлэлд түшиглэн илрүүлнэ.
- ⚠️Хариу үзүүлэх 👷 – Хэрэглэгч, харилцагч эсвэл ажилтан зэргээс зөрчлийн тухайн мэдээлэл авч зөрчилд хариу үзүүлэх процесс эхлэх бөгөөд тухайн иргэний зөрчлийн тохиолдол дээр дараах хариу үзүүлэх алхмуудыг хийж хэрэгжүүлж болох юм. Үүнд:

- Анхны халдлагын векторыг тогтоох;
- Халдагчид ямар арга, хэрэгсэл, тактик хэрэглэж байсныг тодорхойлох;
- Халдагчид хэрхэн байгууллагын сүлжээнд нэвтэрснийг судлах;
- Анхан шатны зөрчлийг шийдвэрлэхтэй холбоотой зөвлөмж өгөх, жишээ нь нууц үгээ яаралтай солих гэх мэт.

🇲🇳 📌Манай Монгол улсад кибер аюулгүй байдлын тухай[1] хууль батлагдсанаар дээр дурдсан CERT/CSIRT-ийн үндсэн чиг үүргийг гүйцэтгэх кибер халдлага, зөрчилтэй тэмцэх Үндэсний төв, Зэвсэгт хүчний төв, Нийтийн төв гэсэн 3 төвүүдтэй болсон бөгөөд тэдгээр нь чиг үүрэг болон хамрах хүрээгээрээ ялгаатай.

Кибер халдлага, зөрчилтэй тэмцэх нийтийн төв буюу PublicCSIRT/CC-ын хувьд онц чухал мэдээллийн дэд бүтэцтэй хувийн хэвшлийн хуулийн этгээд болон төрийн мэдээллийн нэгдсэн сүлжээнд холбогдсон байгууллагаас бусад иргэн, хуулийн этгээдийн мэдээллийн систем, мэдээллийн сүлжээнд чиглэсэн кибер халдлага, зөрчлийг илрүүлэх, таслан зогсоох, хариу арга хэмжээ авах, кибер халдлага, зөрчилд өртсөн мэдээллийн системийг нөхөн сэргээхэд дэмжлэг үзүүлэх үндсэн үүрэгтэй. Мөн кибер халдлага, зөрчлийн талаар судалгаа, дүн шинжилгээ хийх, олон нийтэд зөвлөмж, мэдээлэл түгээх, иргэн, хуулийн этгээдэд кибер халдлага, зөрчлийн талаар зөвлөмж, шаардлага хүргүүлэх чиг үүрэг бүхий байгууллага юм. Дээрх чиг үүргийг хүрээнд хийж гүйцэтгэх үйл ажиллагааг нь хууль дүрэмд[2] заасан байдаг ба нийтийн төв нь иргэн танд дараах байдлаар туслалцаа үзүүлэх боломжтой. Үүнд:

- 🤝Мэдээллийн систем, мэдээллийн сүлжээний аюулгүй байдлын талаар зөвлөмж өгөх;
- 🤝Кибер халдлага, зөрчлийн талаар мэдээлэл хүлээн авах, шалгаж шийдвэрлэх;
- 🤝Мэдээллийн систем, мэдээллийн сүлжээнд чиглэсэн кибер халдлага, зөрчилд хариу арга хэмжээ авах болон мэдээллийн системийг нөхөн сэргээхэд мэргэжлийн арга зүйн туслалцаа, дэмжлэг үзүүлэх.

[1] Монгол улсын хууль – Кибер аюулгүй байдлын тухай хууль
[2] Монгол улсын засгийн газрын тогтоол – Хавсралт – “Кибер халдлага зөрчилтэй тэмцэх нийтийн төв” улсын төсөвт үйлдвэрийн газрын дүрэм

📞📢Мөн таны кибер аюулгүй байдалд тулгарсан асуудлыг шийдвэрлэхэд үүрэг оролцоотой тухайлсан чиг үүргийн байгууллагууд байдаг. Хэрэв та аль байгууллагад мэдэгдэхээ мэдэхгүй байгаа бол Кибер халдлага, зөрчилтэй тэмцэх нийтийн төвтэй холбогдон лавлах боломжтой. Тухайлбал:

- ❓ Хэрэв та эрүүгийн гэмт хэрэг, тухайлбал, цахим залилан, санхүүгийн хохирол учруулсан хэргийн талаар мэдээлэхийг хүсвэл Цагдаагийн ерөнхий газрын цахим гэмт хэрэгтэй тэмцэх газарт хандах боломжтой.
- ❓ Мөн, хэрэв таны онлайн банк болон картын мэдээлэл алдагдсан бол холбогдох банк, санхүүгийн байгууллагатай яаралтай холбоо барих нь зүйтэй.
- ❓ Хэрэв та интернэтийн үйлчилгээний доголдлыг мэдээлэхийг хүсвэл холбогдох үйлчилгээ үзүүлэгч байгууллагатай холбоо бариарай.

Кибер халдлага, зөрчилтэй тэмцэх нийтийн төв нь Кибер аюулгүй байдлын тухай хууль, болон холбогдох дүрэм, журамд заасан хамрах хүрээ, үүрэг чиглэлийн хүрээнд үнэ төлбөргүй үйлчилгээ үзүүлдэг. Тиймээс хэрвээ танд кибер зөрчил тохиолдвол нийтийн төвд хандан хэрхэн хариу үзүүлэх талаар зөвлөгөө, тусламж авч болох бөгөөд ингэснээр зөрчилд хариу үзүүлэх хугацааг богиносгож, илүү их хохирол учрахаас сэргийлж болох юм шүү.

Хамрах хугацаа:	**2024 оны 7-р сарын сүүлийн хагас (#2)**
Хамрах сэдэв:	**Кибер зөрчлийн бодит түүх болон түүнийг шийдвэрлэсэн арга зам, мөн түүнчлэн кибер зөрчлийг мэдээлэх зөвлөмж (КАБ-ын хуулийн 18.2 заалтыг сануулах)**

📌⚠️**Кибер зөрчлийн бодит түүх болон түүнийг шийдвэрлэсэн арга зам:**

💸 👾 2017 оны 5-р сард дэлхий даяар тархсан томоохон кибер халдлагын бодит түүх болох WannaCry рансомвэйрын тухай хуваалцъя. Энэ халдлага нь Microsoft Windows үйлдлийн системийн EternalBlue эмзэг байдлыг ашиглан маш хурдан тархсан ба 150 гаруй улс орны 230,000 гаруй компьютерт халдаж, маш олон байгууллагуудыг хохироосон бөгөөд эрүүл мэнд, тээвэр, банк зэрэг олон салбарт нөлөөлсөн. Энэхүү кибер зөрчлийг шийдвэрлэхэд олон улсын CERT-үүд болон бусад кибер аюулгүй байдлын байгууллагууд хамтран ажилласан байдаг. Уг халдлага буюу кибер зөрчлийг дараах арга замаар шийдвэрлэсэн.

1. 🔎 Анхан шатны хариу арга хэмжээ 🚨:

- ⚠️⚙️ Эмзэг байдлыг илрүүлэх, мэдээлэх: Microsoft нь EternalBlue эмзэг байдлыг илрүүлж, халдлагаас өмнө patch буюу засварыг гаргасан байсан боловч олон байгууллага энэ засварыг суулгаагүй байсан.
- ⚠️👾 Халдлагыг илрүүлэх: Мэдээлэл аюулгүй байдлын байгууллагууд халдлагыг анх илрүүлж, холбогдох талуудад сэрэмжлүүлсэн.

2. 🔒 Зөрчлийг хязгаарлах, эрсдэлийг бууруулах ⬇️:
   - 💻🚧 Системүүдийг тусгаарлах: Халдвар авсан системүүдийг сүлжээнээс салгаж, тархалтыг зогсоох арга хэмжээг авсан.
   - 🔄🩹 Засвар болон шинэчлэлт: Microsoft-ийн гаргасан засвар болон шинэчлэлтийг яаралтай хэрэгжүүлсэн.
3. 🔍 Шинжилгээ, судалгаа 📊:
   - 💥🔍 Халдлагын судалгаа: Халдлагын механизм, тархалтын арга техникийг судалж, хортой кодын үйл ажиллагааг нарийвчлан шинжилсэн.
   - 🤝📈 Мэдээллийн солилцоо: Олон улсын CERT-үүд болон кибер аюулгүй байдлын байгууллагууд хамтран мэдээлэл солилцож, халдлагын талаарх мэдээллийг хурдан тараасан.
4. 🔄 Нөхөн сэргээх үйл ажиллагаа 🛡️:
   - 📂🔧 Файлуудыг сэргээх: Шифрлэгдсэн файлуудыг сэргээх арга хэмжээ авсан бөгөөд зарим байгууллагууд өгөдлийн нөөц хувилбарыг ашиглан файлуудаа сэргээсэн.
   - ⚙️🔧 Системүүдийг цэвэрлэх: Халдвар авсан системүүдийг цэвэрлэж, хэвийн үйл ажиллагааг сэргээсэн.
5. 💡 Олж авсан туршлагаасаа суралцах 📝:
   - 📑🔄 Бодлого, журмаа шинэчлэх: Олон байгууллагууд аюулгүй байдлын бодлого, журмаа шинэчилж, аюулгүй байдлын шинэ арга хэмжээнүүдийг хэрэгжүүлсэн.
   - 💡🤝 Сургалт, мэдлэг олгох: Ажилтнуудыг аюулгүй байдлын талаар сургаж, мэдлэг олгох үйл ажиллагааг өргөжүүлсэн.

Энэхүү зөрчилд хариу үзүүлэх үйл ажиллагаанд CERT-үүд дараах үүрэг оролцоотой байсан.

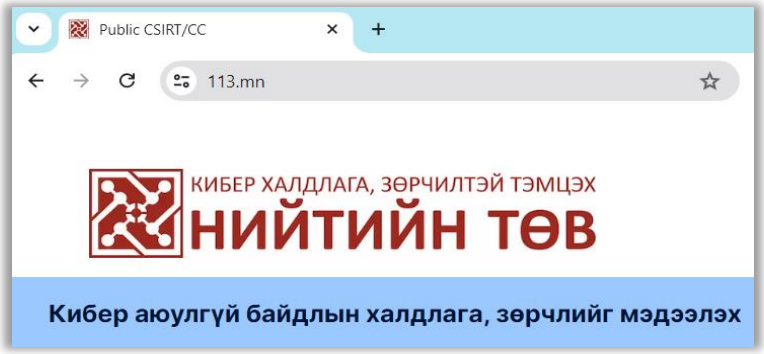
- Мэдээлэл түгээх: Халдлагын талаар мэдээллийг хурдан тарааж, холбогдох байгууллагуудад сэрэмжлүүлэх.
- Зөвлөмж гаргах 🎯 : Халдлагаас хамгаалах зөвлөмж, арга хэмжээг гаргах.
- Хамтын ажиллагааг хэрэгжүүлэх🤝:Олон улсын болон үндэсний хэмжээнд хамтран ажиллаж, халдлагыг хязгаарлах, арилгахад оролцох.

WannaCry халдлага нь олон улсын CERT-үүдийн хамтын ажиллагаа, мэдээлэл солилцооны ач холбогдлыг тодруулж, кибер аюулгүй байдлын арга хэмжээнүүдийг

сайжруулахад нөлөө үзүүлсэн томоохон халдлага зөрчлийн тохиолдол байсан.

📌 ⚠️ **Кибер зөрчлийг мэдээлэх зөвлөмж:**

⚖️Өмнөх агуулга дээр дурдаж байснаар манай улс кибер аюулгүй байдлын тухай хуультай болсноор кибер халдлага зөрчилтэй тэмцэх төвүүдтэй болсон билээ. Тэдгээр төвүүдээс

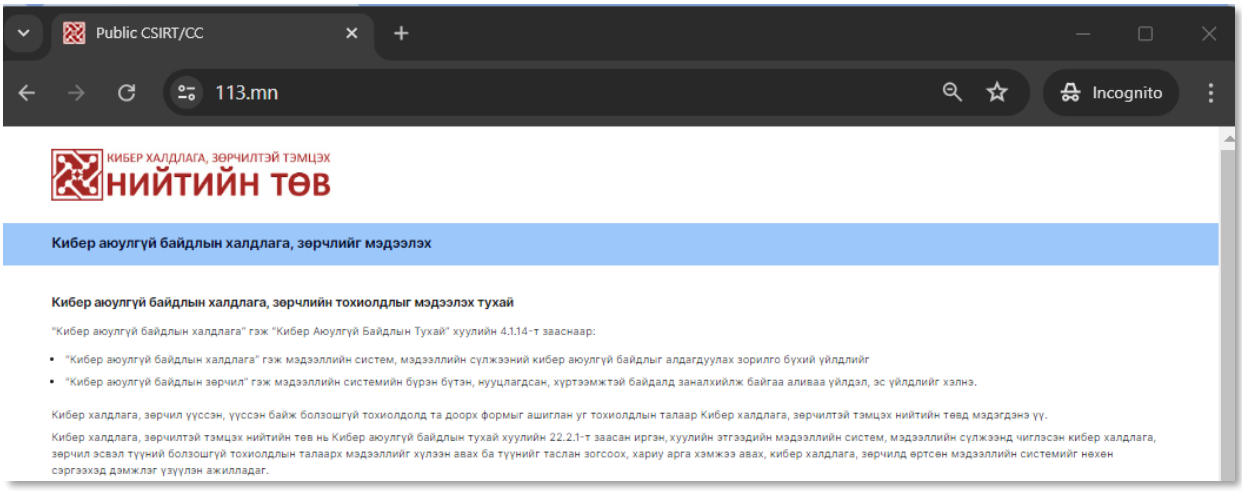


кибер халдлага, зөрчилтэй тэмцэх нийтийн төв нь Кибер аюулгүй байдлын тухай хуулийн 22.2.1-т заасан иргэн, хуулийн этгээдийн мэдээллийн систем, мэдээллийн сүлжээнд чиглэсэн кибер халдлага, зөрчил эсвэл түүний болзошгүй тохиолдлын талаарх мэдээллийг хүлээн авах ба түүнийг таслан зогсоох, хариу арга хэмжээ авах, кибер халдлага, зөрчилд өртсөн мэдээллийн системийг нөхөн сэргээхэд дэмжлэг үзүүлэн ажилладаг. Мөн уг хуулийн 18.2 заалтад “Кибер халдлага, зөрчил үүссэн, үүссэн байж болзошгүй тохиолдолд Нийтийн төвд даруй мэдэгдэж болно” хэмээн тусгасан байдаг. Тиймээс хэрвээ танд ямар нэг кибер зөрчил тохиолдсон бол Нийтийн төвийн кибер аюулгүй байдлын халдлага, зөрчлийг мэдээлэх 🌐 https://113.mn/ сайтад хандан зөрчлийн талаар мэдээлэх боломжтой. Мөн 📞113 тусгай дугаарт хандан мэдээлж болно.

ЖИШЭЭ ЗААВАРЧИЛГАА

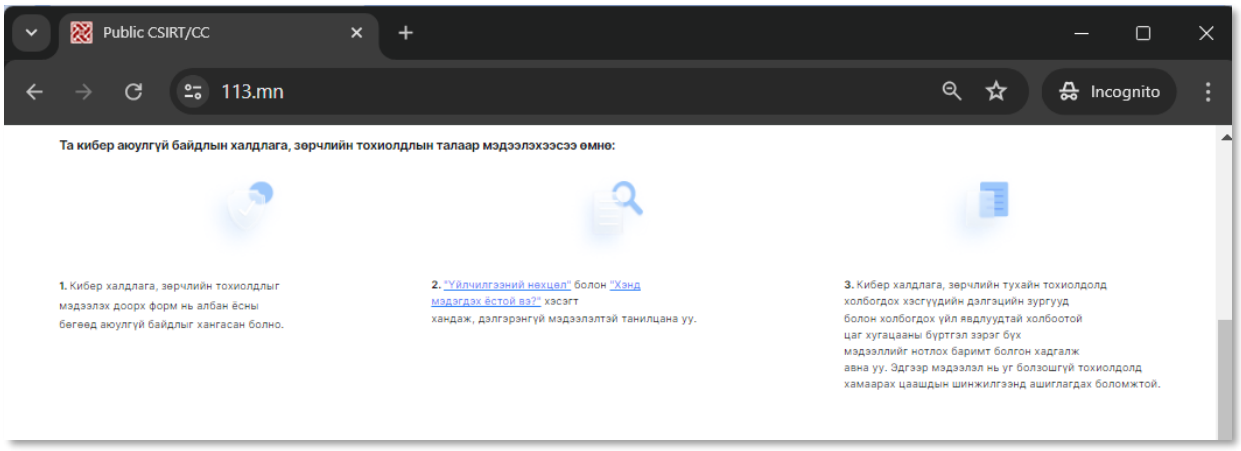
Кибер халдлага, зөрчилтэй тэмцэх нийтийн төвийн дэргэдэх Кибер аюулгүй байдлын халдлага, зөрчлийг мэдээлэх https://113.mn/ сайт дээр зөрчлийн талаар хэрхэн мэдээлэх тухай тайлбарлая.

1. Эхлээд кибер аюулгүй байдлын халдлага, зөрчлийн тохиолдлыг мэдээлэх тухай хэсгээс кибер зөрчлийг мэдээлэх, мэргэжлийн туслалцаа авах хууль эрх зүйн үндэс болон үүнд хамаарах Нийтийн төвийн чиг үүргийн талаарх танилцах боломжтой.



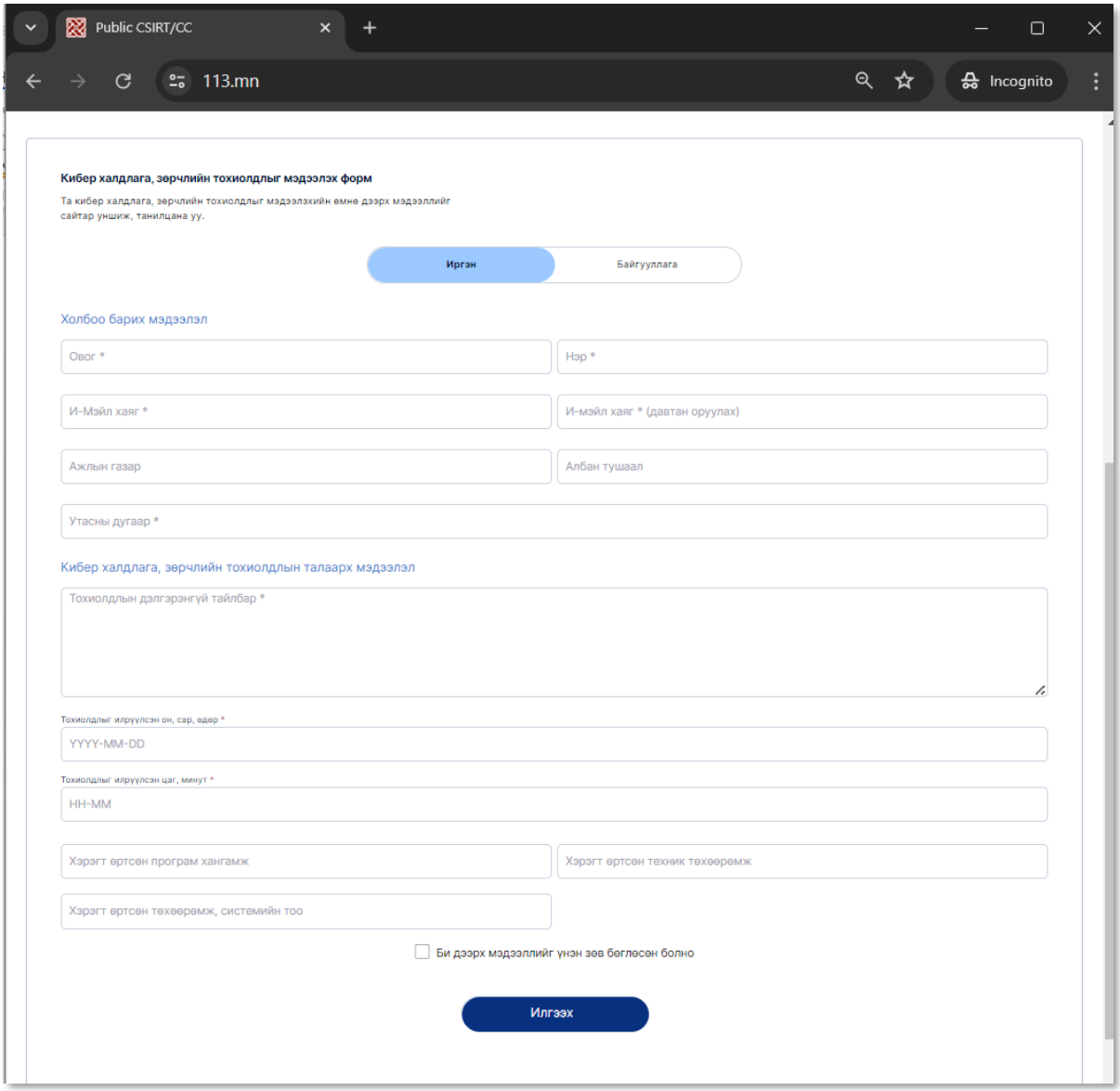
Зураг 1. https://113.mn/ сайтын интерфэйс - Кибер аюулгүй байдлын халдлага, зөрчлийн тохиолдлыг мэдээлэх тухай хэсэг

2. Дараа нь кибер аюулгүй байдлын халдлага, зөрчлийн тохиолдлын талаар мэдээлэхээсээ өмнө анхаарвал зохих зүйлсийн талаар сайтар танилцаарай.

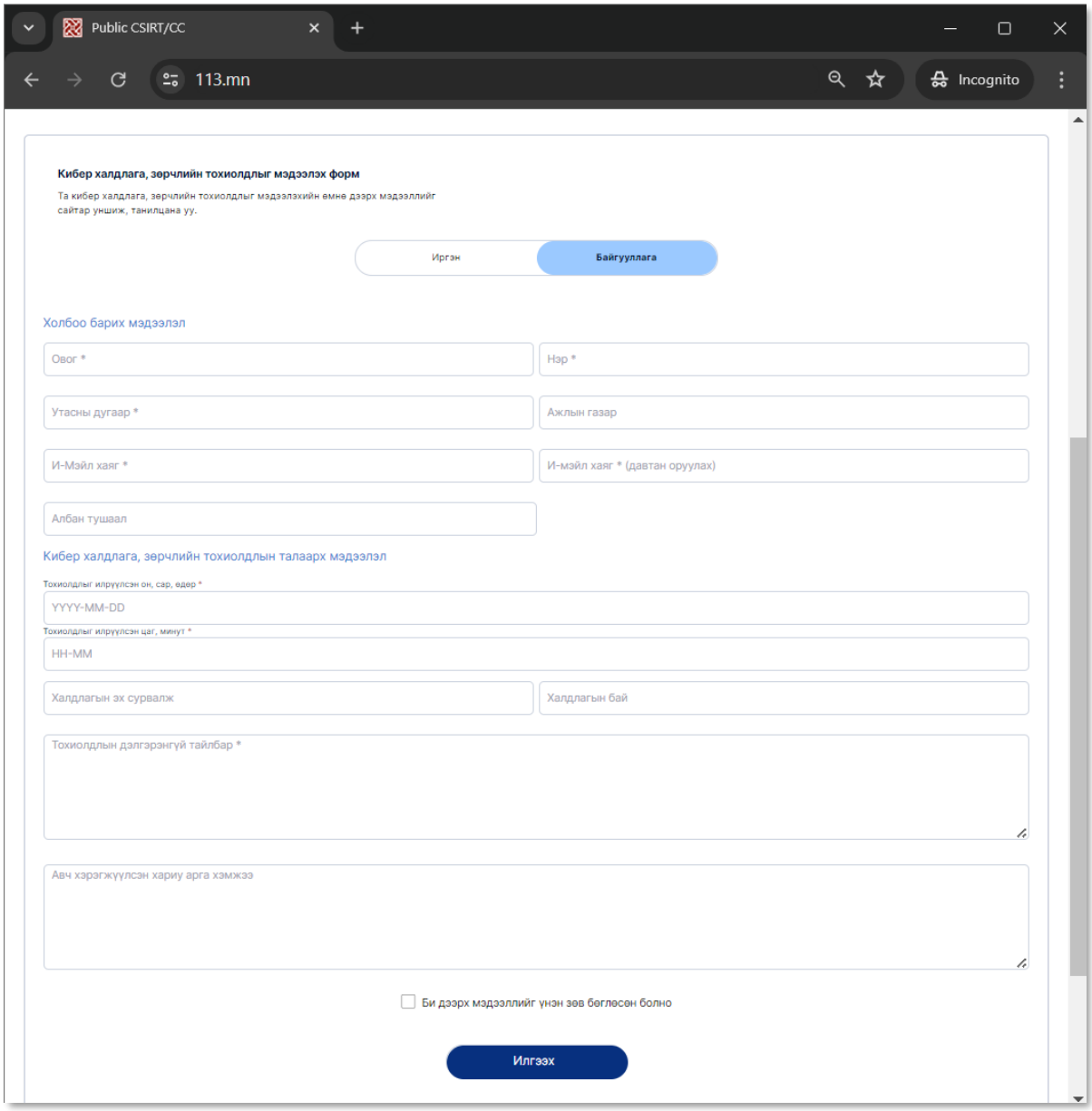


Зураг 2. https://113.mn/ сайтын интерфэйс - кибер аюулгүй байдлын халдлага, зөрчлийн тохиолдлын талаар мэдээлэхээсээ өмнө танилцах хэсэг

3. Дээр дурдсан хэсгүүддээ танилцаж, тодорхой ойлголттой болсны дараа дараа кибер халдлага, зөрчлийн тохиолдлыг мэдээлэх формыг бөглөнө. Ингэхдээ иргэн, байгууллага гэсэн сонголтоос өөрт тохирох сонголтыг хийж, зохих мэдээллүүдийг үнэн зөв бөглөж оруулна. Хамгийн гол нь уг формыг үнэн зөв бөглөх бөгөөд үнэн зөв бөглөснөө баталж checkbox-ыг сонгосноор таны зөрчлийн тухай мэдээлэл цааш илгээгдэх боломжтой болно.



Зураг 3. Иргэний бөглөх форм



Зураг 4. Байгууллагын бөглөх форм

Зөрчлийн талаар Нийтийн төвд мэдэгдэхээс гадна зөрчлийн тухайн тохиолдолд холбогдох хэсгүүдийн дэлгэцийн зургууд болон холбогдох үйл явдлуудтай холбоотой цаг хугацааны бүртгэл зэрэг бүх мэдээллийг нотлох баримт болгон хадгалж авах нэн чухал гэдгийг дахин онцолъё. Эдгээр мэдээлэл нь уг болзошгүй тохиолдолд хамаарах цаашдын шинжилгээнд ашиглагдах боломжтой байдаг.

Мөн түүнчлэн, зөрчлийн хор хохирлыг бууруулахын тулд дараах алхмуудыг авч хэрэгжүүлэх нь зүйтэй. Үүнд:

1. Зөрчлийн шинж тэмдгийг олж харах
   - Компьютер тань хэвийн бус ажиллах (удаашрах, гэнэт мессежнүүд гарч ирэх).
   - Суулгаагүй файл эсвэл программууд гарч ирэх.

- Хувийн мэдээллийг тань авахыг хүссэн имэйлүүд ирэх.

2. Хэрэв ямар нэг зүйл буруу санагдвал дараах үйлдлүүдийг хийх.
   - Интернэтээ салгах - Сүлжээний кабелийг салгах эсвэл Wi-Fi-г унтраах.
   - Сэжигтэй файлыг нээхгүй байх – Мэдэхгүй байгаа файл, программыг нээж, устгаж, зөөж болохгүй.
3. Хаяг бүртгэлээ хамгаалаах
   - Нууц үгээ нэн даруй солих. Ингэхдээ хүчтэй нууц үг үүсгэх (Том, жижиг үсэг, тоо, тэмдэгтийн холимог).
   - Хоёр хүчин зүйлт баталгаажуулалтыг идэвхжүүлэх (хамгаалалтын нэмэлт алхам).
4. Онлайн орчинд аюулгүй байх
   - Компьютер болон программуудаа шинэчлэх.
   - Танихгүй хүмүүсээс ирсэн имэйл болон холбооснууд дээр шууд дарахгүй байх.
   - Чухал файлуудыг тогтмол нөөцөлж авах.
5. Мэргэжилтнүүдийн өгсөн зааварчилгаа, зөвлөгөөг дагах
   - Танаас ямар нэгэн хэрэгсэл ажиллуулах эсвэл таны компьютерт хандах эрх олгохыг хүсвэл зөвшөөрөх.
   - Танд нууц үгээ солихыг зөвлөвөл түүний дагуу нууц үгээ солих.

ДҮГНЭЛТ

Зөвхөн манай улсад гэлтгүй дэлхий даяар кибер халдлага өсөн нэмэгдэж байгаа бөгөөд гарч болох зөрчлийн хор хохирлыг бууруулах хамгийн үр дүнтэй арга бол зөрчилд хурдан хариу үзүүлэх явдал юм. IBM Security 2023[3] оны судалгаа дээр дурдагдсанаар зөрчилд 30 хоногийн дотор хариу үзүүлэх нь үүнээс удаан хугацаанд хариу үзүүлж буй байгууллагуудтай харьцуулахад дунджаар 1 сая ам.доллар хэмнэдэг гэсэн тоо гарсан байсан. Харин зөрчилд хариу үзүүлэх процессын бэлтгэх үе нь чухал гэдгийг Понемон институтийн 2020[4] оны судалгаа дээр харуулсан байсан ба зөрчилд хариу үзүүлэх төлөвлөгөөтэй байгууллагууд төлөвлөгөөгүй байгууллагуудтай харьцуулахад нэг мэдээллийн алдагдал зөрчил дээр дунджаар 2.66 сая ам.долларoop хохирлоо бууруулж чаддаг гэсэн байв. Тэгэхээр эдгээр тоон дээрээс бид зөрчлийн учруулж болзошгүй хор хохирлыг бууруулахад зөрчилд хариу үзүүлэхэд бэлэн байх болон зөрчилд аль болох хурдан хариу үзүүлэхийн чухлыг харж болох юм. Тиймээс танд ямар нэг кибер зөрчил тохиолдвол мэргэжлийн хүмүүст хандаж зөвлөгөө тусламж аваарай. Ингэснээр тухайн мэргэжилтнүүд зөвхөн таны тохиолдолд туслаад зогсохгүй, тухайн зөрчил дээр дүн шинжилгээ хийж, мөн уг зөрчлийн тохиолдол нь бусдад тохиолдохоос сэргийлэх арга хэмжээг хэрэгжүүлэх боломжтой болох юм. Мөн та мэргэжлийн байгууллагаас өгч буй мэдээ мэдээлэлтэй танилцаж, кибер аюул занал, халдлагуудын талаар мэдлэг, мэдээлэлтэй байгаарай.

ОЙЛГОЛТ ШАЛГАХ АСУУЛТУУД

[3] IBM security - https://www.ibm.com/reports/data-breach
[4] Ponemon Institute research - https://shorturl.at/cwjVZ

1. Кибер зөрчилд хариу үзүүлэх үйл ажиллагааны үндсэн зорилго юу вэ?
   a) Программ хангамжийн шинэ боломжуудыг хөгжүүлэх
   b) Олон нийттэй харилцах харилцааг зохицуулах
   c) Учирч болох хохирлыг бууруулах, зөрчлөөс хурдан нөхөн сэргэх боломжтой болгох
   d) Ажилчдын тоог цөөлөх
2. Кибер зөрчилд хариу үзүүлэх багийн (CERT/CSIRT) үндсэн зорилго юу вэ?
   a) Шинэ программ хангамжийн хэрэглэж турших
   b) Кибер зөрчлийг зохицуулах, хариу арга хэмжээ авах
   c) Компанийн маркетингийн стратегийг удирдах
   d) Бүтээгдэхүүний асуудал дээр хэрэглэгчдэд дэмжлэг үзүүлэх
3. Та ямар үед кибер халдлага, зөрчилтэй тэмцэх нийтийн төвд хандах хэрэгтэй/боломжтой вэ?
   a) Банкны картын мэдээлээ алдсан тохиолдолд
   b) Цахим залилангийн хохирогч болсон тохиолдолд
   c) Төхөөрөмж дээр программ суулгахад тусламж хэрэгтэй үед
   d) Кибер халдлага, зөрчил үүссэн эсвэл үүссэн байж болзошгүй тохиолдолд
4. Кибер халдлага, зөрчилтэй тэмцэх нийтийн төвийн тусгай дугаар хэд вэ?
   a) 111
   b) 112
   c) 113
   d) 114
5. Кибер зөрчлийн талаар холбогдох байгууллагад мэдээлсний дараа юу хийх ёстой вэ?
   a) Цаашид арга хэмжээ авахгүйгээр засаж өгөхийг нь хүлээх
   b) Олон нийтийн мэдээллийн хэрэгслээр үйл явдлын талаарх бүх мэдээллийг нийтэд түгээх
   c) Тэдний зөвлөмжийг дагаж, өгөгдөл, системээ хамгаалах арга хэмжээ авах
   d) Утасны дугаараа солих