НЭЭЛТТЭЙ
НИЙГЭМ
ФОРУМ

Иргэний нийгмийнхэнд зориулсан мэдээллийн аюулгүй байдлын анхан шатны сургалтын гарын авлагатай танилцана уу.

Цахим халдлага гэж юу вэ?
Цахим халдлага нь хэрэглэгчийн хувийн болон нууц мэдээллийг олзлон авч ашиг хонжоо олоход ашиглах зорилготой гэмт үйлдэл юм. Ихэнх цахим халдлага компьютерын сүлжээ, системд халдах, эсвэл хэрэглэгчийг сэрэмж алдуулан мэдээллээ задлахад хүргэх гэсэн хоёр арга замаар үйлддэгдэг.

Цахим халдлагын зорилго?
1) Ихэнх тохиолдолд хувь хэрэглэгч хүн рүү чиглэсэн, хувийн болон нууц мэдээлэл (жишээлбэл, банкны дансны мэдээлэл, хадгалсан хувийн зураг, нууц үг гэх мэт)-ийг олж аваад, ашиг хонжоо хайх нь хамгийн нийтлэг зорилго. Зарим жишээг дурдвал таны нэрийг барин цахим шуудангаар мөнгө залилж авах, таны болон байгууллагын тань нэр хүндийг унагах утга агуулгатай захидал тараах, нууц мэдээллийг тараахаар сүрдүүлж мөнгө нэхэх.
2) Зарим нь бизнесийн өрсөлдөгчийн эсрэг, мөн улс төрийн зорилготой халдлага байдаг. Жишээлбэл, интернэтээр үйлчилгээ эрхэлдэг байгууллага, төрийн байгууллагын вебсайтын нууцлалыг эвдэж нээх боломжгүй болгоод мөнгө нэхэх, хамгаалалт муутай байгааг харуулах.
3) Эдгээр халдлагын зарим нь хакеруудын дунд ур чадвараа гайхуулж алдар нэр олох зорилготой.

Улмаар цахим халдлага нь тодорхой нэг хүний эсрэг зохион байгуулалттай, зорилтот үйл ажиллагаа байх нь ховор, харин дийлэнхдээ урхинд орж хууртагдан нууц болон хувийн мэдээллээ өөрөө өгөх хэрэглэгчийг отож байдаг эрсдэл юм.

Цахим халдлагын төрөл хэлбэр
Цахим халдлагыг ерөнхийдөө 7 төрөлд ангилж болох бөгөөд эдгээрийн 6 нь техникийн шинжтэй, нэг нь хүний сэтгэл зүйд суурилсан нийгмийн инженерчлэл хэмээх арга болно.

1) **Бидний хэлж сурснаар вирус** болоод бусад компьютерын хортой, аюултай программууд нь таны ухаалаг төхөөрөмжид “сууж” сөрөг нөлөө үзүүлдэг. Хэлбэрээсээ үл хамааран эдгээр аюултай программ нь интернет сүлжээгээр, хавсаргасан имэйл файлаар, холбоосоор, мөн флашаар гэх мэт зөөврийн системээр дамжиж таны ухаалаг төхөөрөмжид “сууна”.
2) **Фишинг/Дэгээ хаях** гэх (англиар “fishing” буюу загасчлах гэсэн үгтэй утга нэг) арга нь загасчлахтай ижил үе шатаар хэрэгждэг. Цахим шуудан, месеж, харилцааны өөр ямар нэг системээр таны сэтгэл зүйд нөлөөлж нууц үгээ өөрөө хэлээд өгөхөд хүргэх “өгөөш” явуулснаар фишинг төрлийн дайралт эхэлдэг.
3) **Нууц үг тааруулах:** Нууц үг бол таны цахим түлхүүр юм. Хурд сайтай компьютер, үгийн сан ихтэй мэдээллийн бааз хоёрыг ашиглан нууц үгийг таах биш тааруулж болно.
4) **Дундын этгээд болох (дүрд тоглох арга):** Та банкны хүнтэй чатаар харилцаж байхад гуравдагч этгээд дундаас нь тагнан сонсон, мэдээллийг хуулж авна. Тагнуулын ажиллагаа юм шиг санагдаж болох ч амьдрал дээр хамаагүй энгийн аргаар хэрэгжүүлж болох зүйл юм. Жишээлбэл, олон нийтийн орчинд үнэгүй WiFi ашиглах бүртээ та хамгаалагдаагүй сүлжээнд орж байгаа бөгөөд энэ сүлжээг ашиглан та банкны апп руугаа нэвтэрсэн бол таны мэдээллийг хамгаалалтгүй энэ сүлжээнд байж байгаа нэг хакер дундаас нь хуулж авах боломжтой.
5) **Үйлчилгээг хаах:** Энэ арга нь хувь хэрэглэгч бус, харин вэбээр дамжуулан үйлчилгээ эрхэлдэг байгууллагад хамаатай. Халдагч тухайн байгууллагын цахим хуудсаар хүчин чадлаас нь ахадсан өндөр ачааллыг үүсгэх бот ажиллуулснаар вебийн сүлжээ унах, хаагдах, цаашлаад төхөөрөмж шатах аюултай. Байгууллагаас мөнгө нэхэх, бизнесийн болон улс төрийн өрсөлдөгч байгууллагын нэр хүндийг унагах зорилгоор энэ халдлагыг ашиглах нь их байдаг.
6) **Drive-by Downloads:** танаас зөвшөөрөл асуухгүйгээр ухаалаг төхөөрөмжид тань “суудаг” программууд байдаг бөгөөд эдгээр нь таны тухайн ухаалаг төхөөрөмжийг ашиглан дамжуулж байгаа бүх мэдээллийг хуулж аваад, халдагч этгээдэд дамжуулж байхаар зохиогдсон байдаг. Эдгээр нь мөн л таныг мөшгөж мөрдөхөөс илүүтэй нууц үг, нууц мэдээлэл, хувийн мэдээлэл зэрэг ашиг хонжоо олоход ашиглаж болох мэдээллийг олзлох зорилготой.

7) **Нийгмийн инженерчлэл** гэж хүнийг бодож тунгаах боломжгүй нөхцөл үүсгэн, нууц үг, нууц мэдээллийг хэлүүлж авах, ухаалаг төхөөрөмжийнх нь хамгаалалтыг өөрөөр нь унтраалган нэвтрэх боломж олж авах зорилготой арга заль юм. Яг одоо, 2 минутын дотор, эхний 10 хүнд гэх мэтээр яаруулж шавдуулах, сугалаанд хожсон тул, данс тань хаагдах гээд байгаа тул, таньдаг хүн тань мөнгө, баримт бичгээ алдаад зовж байгаа тул гэх мэт сэтгэл хөдлөлийг өдөөх замаар рационал бодож тунгаах боломжгүй байдалд оруулах, эсвэл нэр хүнд бүхий байгууллага, хүний нэрийг барих, өнгө төрхийг ашиглах замаар мэхлэх арга хэрэглэдэг. Онцлог нь араас нь таны хэрэглэгчийн нэр + нууц үг, дансны дугаар + нууц үгийг бичих, хэлж өгөх хүсэлт дагалддаг бөгөөд энэ нь цахим халдлагын гол зорилго, танигдах онцлог нь юм.

Цахим аюулгүй байдал бол дээрх арга зальд автахгүй байх, халдлагаас хамгаалах арга хэмжээ авахыг хэлнэ.

Цахим аюулгүй байдлаа хэрхэн хангах юм бэ?
Байгууллага, хүмүүсийн туршлага, мэдлэг, цахим хэрэглээ ялгаатай ч нийтлэгээр дараах 6 арга хэмжээг авах хэрэгтэй:

1. Биет хамгаалалт хангах
2. Программ хангамжийн баталгаатай байдлыг хангах
3. Браузер болон интернэтийн аюулгүй байдлыг хангах
4. Сайн нууц үг, хоёр шаттай баталгаажуулалт ашиглах
5. Фишинг төрлийн халдлагыг таних мэдлэгтэй байх
6. Датагаа back up хийж байх

1) Биет хамгаалалтыг хангах
Notebook дээр жишээ авах юм бол дэлгэц, гар, хулгана, мэдрэгч, сэнс, хард диск гээд ухаалаг төхөөрөмжийн биет хэсгийг хамгаалах

- Төхөөрөмжийн бүх хэсэг бүрэн ажиллагаатай байх
- Хараа хамгаалалтгүй орхих, мартах, хулгайд алдахаас сэргийлэх
- Компьютер дээр ажиллаж байхдаа шингэн зүйл хол байлгах

2) Программ хангамжийн баталгаатай байдлыг хангах

- **Албан ёсны лицензтэй программ ашиглах**

Ухаалаг төхөөрөмжийг ажиллуулдаг программ хангамж буюу үйлдлийн систем нь баталгаатай, найдвартай буюу лицензтэй программ байх шаардлагатай. Лицензгүй программ нь вирус авахаас хамгаалж чадахгүй.

Лиценз яагаад чухал вэ?

a. Ямар ч программ анх гарахдаа жижиг алдаа, сул талуудтай байдаг бөгөөд эдгээр нь хэрэглээний явцад мэдэгддэг. Хакерууд эдгээр сул талыг л ашиглана. Программ хөгжүүлсэн мэргэжлийн байгууллага нь тэр сул талыг засаж залруулах update гаргаж, лицензтэй программ ашиглаж байгаа хэрэглэгчид update-ыг татаж авснаар хэрэглэж байгаа программын сул тал дээр “нөхөөс” тавигдана.
b. Шинэ үеийн үйлдлийн систем гарч лицензтэй программ ашиглаж байгаа хэрэглэгчид үнэгүй update хийх боломжтой. Жишээ: албан ёсны лицензтэй Windows 10 ашиглаж байсан хэрэглэгчид Windows 11 гарахад үнэгүй татаж авах боломжтой

Дэлгүүрээс компьютер худалдаж авсан бол лицензтэй гэж найдаж болохгүй. Монголд “хулгайн” программ их байдаг тул борлуулалтын мэргэжилтнээс лавлаж асуух хэрэгтэй. Нэмэлт төлбөр төлөөд лицензтэй программ суулгаж өгдөг бол худалдаж авах хэрэгтэй. Нэг үеэ бодвол программ хангамж боломжийн үнээр нийлүүлдэг газрууд ч бий болсон.

- **Компьютерын хамгаалалтын систем**.

Хүний биед өөрийгөө гаднын халдвараас сэргийлэх, мөн халдвар илэрсэн үед дарж устгах дархлааны систем байдаг шиг компьютер ч мөн төрөл бүрийн вирус, хортой программын халдвараас урьдчилан сэргийлэх, илэрсэн үед нь олж устгах хамгааллын системтэй байх ёстой. Windows программын **“Defender”** хамгаалалтын систем нь хувь хэрэглэгчдэд боломжийн хамгаалалт болж чадах ч албан байгууллага илүү хүчин чадалтай, хиймэл оюун ухаанд суурилсан орчин үеийн программыг ашиглах хэрэгтэй.

3) Браузер болон интернэтийн аюулгүй байдал

a) Browser бол таны интернет ертөнцөөр аялуулдаг Google Chrome, Mozilla Firefox, Internet Explorer гэх мэт хөтөчүүд юм. Браузерийн зарим тохиргоо мэдээлэл алдах эрсдэл дагуулдаг

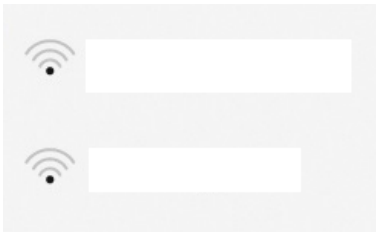
- Browser дээр Remember History, Auto Fill, Save Password зэрэг тохиргоо байдаг нь нэг үйлдлийг олон удаа давтан хийх яршигтай ажлаас хэрэглэгчийг чөлөөлж, орсон хуудасны хаяг, бүртгэлийн мэдээлэл, нууц үгнүүдийг хадгалдаг бөгөөд хакер халдах юм бол таны мэдээлэл задрах аюултай. Ихэнхдээ автоматаар идэвхтэй байдаг эдгээрийг идэвхгүй болгож тохируулаарай.
- Нууц мэдээлэл, онцгой асуудлаар хайлт хийх бол “Private Browsing” хэрэглээрэй. Chrome дээр Incognito хуудсыг нээх, эсвэл SHIFT+CTR+N дарахад шинээр цонх нээгдэн, ажиллаж дуусаад Browser-аа хаахад мэдээлэл хадгалагдахгүй хаана.

b) WiFi:

- Үнэгүй WiFi хамгаалалт сул, төрөл бүрийн халдлагад өртөх эрсдэлтэй тул ийм WiFi хэрэглэхгүй байхыг зөвлөж байна.

Хамгаалалтгүй сүлжээг хэрхэн таних вэ?

Хамгаалалтгүй сүлжээнд байгаа бүх мэдээлэл ямар ч хамгаалалтгүй, задгай байдаг. Энгийнээр, хамгаалалтгүй сүлжээнд холбогдоод банкны мэдээллээ оруулбал таны оруулж байгаа мэдээллийг гуравдагч этгээд харах боломжтой гэсэн үг.



Хамгаалалттай сүлжээнд дамжуулж байгаа мэдээлэл шифрлэгддэг бөгөөд зорилтот хаягтаа хүрсэн үедээ шифр нь тайлагдаад текст болно. Хамгаалалттай сүлжээг жижиг цоожоор нь таньж болно.

Хамгаалалттай сүлжээ байхгүй тохиолдолд утасны 3G/4G дээр Hotspot үүсгэж орох нь илүү аюулгүй.

4) Сайн нууц үг, хоёр шаттай баталгаажуулалт

- Нууц үг гэж юу вэ?

  Та гэртээ ороходоо түлхүүрээр цоожоо нээдэгтэй адил нууц үг бол аливаа систем рүү ороходоо өөрийгөө таниулах хэрэгсэл юм.

- Яагаад та нууц үгэндээ анхаарах ёстой вэ?

  Нууц үг тааруулах халдлага нь том сантай эх сурвалж ашиглаад программ уншуулан, нууц үгийг тохируулдаг. Сайн нууц үг ямар байх талаарх зөвлөмж байнга шинэчлэгдэн, улам нарийн болж байна.

- Сайн нууц үг ямар байх тухай хамгийн сүүлийн үеийн зөвлөмж
  - 16+ тэмдэгтээс бүтсэн байх
  - Том болон жижиг үсэг орсон
  - Тэмдэг орсон (@#$%^&*)
  - Өгүүлбэр хэлбэрээр зохиовол сайн
- Нууц үгтэй зэрэгцүүлэн 2 шаттай баталгаажуулалтын системийг ашиглаж болно. 2 шаттай баталгаажуулалт нь нууц үгээ оруулахаар таны бүртгэлтэй гар утас дээр код ирүүлдэг 2 алхамтай нууц үгийн систем юм. Хоёр шаттай баталгаажуулалт нь систем бүр дээр өөр байдаг, мөн том байгууллагууд өөрийн бие даасан системийг хөгжүүлсэн байдаг (жишээлбэл, Google Authenticator, Microsoft Authenticator, USB key гэх мэт)

5) Фишинг /Өгөөш хаях аргыг хэрхэн таних вэ

Phishing буюу фишинг (англи “Fishing” буюу загасчлах гэсэн үгнээс гаралтай) нь цахим шуудан, бусад харилцааны системээр танд шахалт үзүүлэн, хууран мэхлэх замаар хувийн мэдээллийг авах зорилготой.

Фишинг хэрхэн явагддаг вэ?

- **Өгөөш хаях:** Албан байгууллага, таньдаг хүнээс, чухал үйл явдалтай холбоотой мэйл, чат, утасны мессежээр танд вебийн холбоос, хавсаргасан файл ирнэ.
- **Дэгээг үмхэх:** Танд ирсэн мэдээллийн агуулга нь таныг сандаргах, баярлуулах, эсвэл шуурхай арга хэмжээ авахыг шаардсан өнгө аястай байх тул та бодож тунгаалгүй шууд л үйлдэл хийх яарна.
- **Барьц авах:** Холбоос дээр дараад шууд, заримдаа нэмэлтээр хэрэглэгчийн нэр, нууц үгээ оруулснаар та урхинд орлоо.
- **Хооллох:** Нэгэнт таны бүртгэлийн мэдээлэл халдагчид очсон бол хэрэгтэй мэдээллээ цуглуулж авахад саад болох зүйлгүй.Таны хувийн мэдээлэл алдагдсан байх магадлалтай

Фишинг Жишээ 1: Имэйл

Хэнээс: "Google Support"support@google.corn”

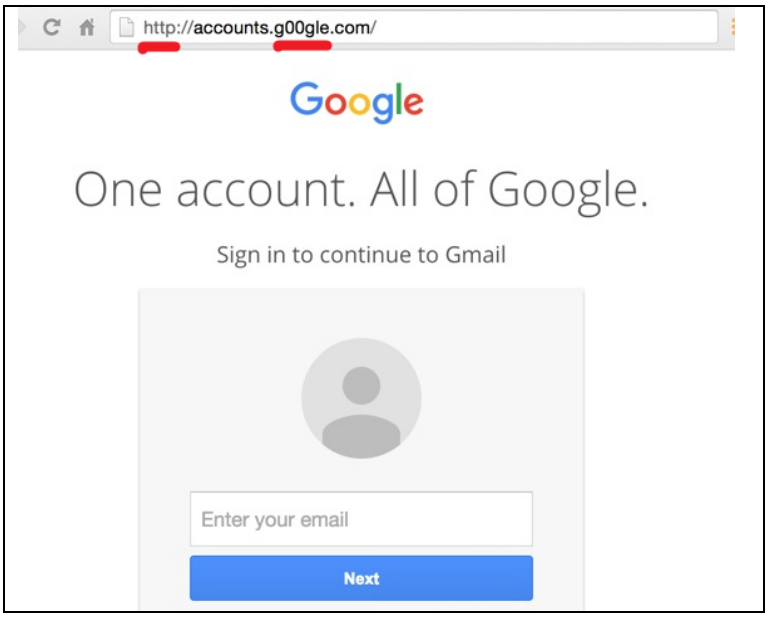
Агуулга: Та яаралтай нууц үгээ шинэчилнэ үү.
Сайн байна уу,

Таны бүртгэлийн нууц үгийн хугацаа 24 цагийн дотор дуусах тул яаралтай доорх холбоосоор нэвтэрч шинэчилнэ үү!!!

Нууц үгээ солих

Жишээ 1-д Гүүлгийн техникийн дэмжлэгийн багаас ирсэн яаралтай захидал мэт харагдах ч хаяг нь google.**com** биш google.**corn**, яаруулж шавдуулсан, мөн нууц үгээ солих холбоос өгсөн байгаа нь хамгийн их сэрэмжлэх ёстой зүйл юм. Та энэ холбоосыг дарвал Гүүглийн цахим хуудас руу биш .corn гэсэн хаягтай газар халдагчийн үүсгэсэн хуудас руу орж, тэнд хэрэглэгчийн нэр, нууц үгээ үлдээх юм. Гүүгл, албан ёсны ямар ч байгууллага хүнд нууц үгээ солих холбоос явуулахгүй бөгөөд таны ашиглаж байгаа аль нэг программын нууц үгийг солих хугацаа болсон бол холбоосоор биш, өөр дээр нь гарч ирэх юм. Холбоос, месеж, утас, чатаар нууц үг солих холбоос ирсэн бол фишинг явж байна гэсэн үг.

Жишээ 2



Линк буюу холбоос дарж мэдээлэл авах нь интернэтийн хэвийн хэрэглээний нэг хэлбэр юм. Өөрөөр хэлбэл, холбоос болгон нь цахим халдлага гэсэн үг биш. Холбоос дараад интернэт хуудас нээсэн бол албан ёсны хуудас мөн гэдгийг баталгаажуулан, Домэйн нэрийг анхаарах хэрэгтэй. Энэ жишээн дээр тайлбарлах юм бол хаягийн хамгийн эхний товчилсон зам нь https буюу secured/ хамгаалагдсан гэсэн тэмдэглэгээтэй байх ёстой.

HTTP:// ≠ HTTPS://

Google.com гэдэг хаягийг албан ёсны Гүүгл компани эзэмшдэг тул түүнтэй адил төстэй харагдаж, хэрэглэгчийн мэхлэх зорилгоор халдагч g00gle.com хаяг үүсгэсэн байна.

..g00gle.com ≠ google.com

6) Дата backup буюу мэдээллийг архивлаж хадгалах

Чухал файлуудаа эрсдэлээс хамгаалж өөр газар хадгалахыг дата backup буюу нөөцлөх гэж нэрлэдэг. Backup хийх 3 арга байна.

- Зөөврийн хард, флаш дээр хуулах
- Үүлэн технологи: найдвартай үүлэн системд өгөгдлөө хадгалах
- Өөр компьютер дээр хадгалах

7) Нийгмийн инженерчлэл

Нийгмийн инженерчлэлийн нэг жишээ бол дээрх фишинг. Хүний нууц болон хувийн мэдээллийг өөрөөр нь хэлүүлж авах цахим халдлагын эдгээр арга нь яг л нүүр тулсан харилцаан дах залилан шиг сониуч зан, бусдад туслах хүсэл, ашиг олох эрмэлзэл зэрэг хүн бүрт байдаг мөн чанарын ашиглан хийгддэг. Үүнээс өөрийгөө хамгаалахын тулд хэрсүү бай.

Хэрсүү цахим хэрэглэгч нь ирсэн хүсэлт, мэдээллийг шалгаж, нягтлан, үнэн зөв мэдээлэл мөн гэдгийг баталгаажуулсны дараа хариулах арга хандлагатай байна. Мэдээллийг нягтлахад дараах энгийн алхмууд тус болно.

- **Эх сурвалжийг шалга**: Энэ захидал, хүсэлт, мэдээлэлд шууд хариу өгөхөөсөө өмнө ямар эх сурвалжаас ирж байгаа тухай бодох. Цахим шуудан бол хаяг нь зөв гэдгийг шалгах, ялангуяа хавсаргасан файл, холбосон линк байх юм бол фишинг биш гэдгийг заавал баталгаажуулах хэрэгтэй.

- **Шууд хариу өгөлгүй нягтал**: Цахим залилан, нийгмийн инженерчлэл нь хүний яаруулж шавдуулах, бодох цаг олгохгүй шууд хариу өгөхөд түлхэх аргуудыг ашигладаг. Үйл явдалд авталгүй, мэдээллийг өөрөө нягтлах хэрэгтэй. Найз, таньдаг хүн чинь чатаар, утсаар мөнгө хүсэх юм бол мөнгө шилжүүлэхээсээ өмнө тэр найз руугаа залгаад лавлаарай. Албан байгууллагаас таны хувийн мэдээллийг утсаар хүсэх юм бол шууд хариу өгөлгүй, өөрөө тэр байгууллагын вебсайт руу орж, эсвэл албан тушаалтан руу нь залгаж лавлаарай.

- **Бодитой эсэх тухай бод**: Ийм зүйл үнэхээр тохиолдох боломжтой юу гэж өөрөөсөө асуугаарай. Найз тань гадаад улсад мөнгөгүй гацсан, танаас өөр туслах хүн байхгүй, эсвэл нэгэн улсын хаан танд л мөнгөө өвлүүлэх гээд байгаа нь хэр бодитой, байж болох зүйл вэ? Чатаар танилцаад, хэсэг хугацааны дараа тантай гэрлэх хүсэлтэй ч Монголд ирэх онгоцны билет авах мөнгө нь хүрэхгүй байгаа тэр хүн хэн болох, юу хийдэг, хаана амьдардаг гээд түүний тухай наад захын зүйлийг та баттай мэдэх үү?