🛡 СОШИАЛ ИНЖЕНЕРЧЛЭЛИЙН НУУЦЫГ ИЛЧИЛЬЕ 🌐

УДИРТГАЛ

Харилцан холбогдсон цахим орчин дахь кибер аюулгүй байдлын хамгийн сул холбоос нь эмзэг байдалтай программ хангамж, сүлжээний тохиргоо бус харин түүнийг ашиглаж байгаа хүн байдаг билээ. Сошиал инженерчлэл нь хүний сэтгэл зүй, сэтгэл хөдлөлд тулгуурлан систем болон өгөгдөлд зөвшөөрөлгүй нэвтрэх зорилготойгоор үйлдэгддэг халдлага юм. Иймд сошиал инженерчлэлийн халдлагын төрлүүдийг таньж, түүнээс сэргийлэхэд туслах зөвлөмжүүдийг танд хүргэе.

ҮНДСЭН АГУУЛГА

Хамрах хугацаа:	**2024 оны 2-р сарын эхний хагас (#1)**
Хамрах сэдэв:	**Сошиал инженерчлэлийн халдлагаас сэргийлэхийн тулд мэдвэл зохих зүйлс**

📌 Сошиал инженерчлэлийн халдлагын шинжүүд болон учруулж болох эрсдэлийг ойлгох нь

Сошиал инженерчлэлийн халдлага нь цахим аюулгүй байдлын хамгаалалтыг давж, шууд программ хангамж, сүлжээ рүү халдлага хийхгүйгээр хүн рүү чиглэж, хүмүүсийн итгэлийг олж авах эсвэл сэтгэл зүй, зан авир цахим хэрэглээний зан үйл дээр тулгуурлан тэдний эмзэг нууцлалтай мэдээлэл болон ашигладаг сошиал платформ, систем рүү зөвшөөрөлгүй хандалт хийх байдлаар үйлдэгддэг. Сошиал инженерчлэлийн халдлагыг е-майл, утасны дуудлага, чат болон бодит харилцан яриа зэрэг хүнтэй харилцаж болох бүхий л сувгийг ашиглан хийдэг. Энэ төрлийн халдлагын гол зорилго нь хүний цахим аюулгүй байдлын мэдлэг сул талыг ашиглан тэдгээрийн итгэлийг олж авах замаар тогтмол ашигладаг веб хуудаснуудыг нь дуурайлган хийж мэхлэх замаар хэрэглэгчийн нэр, нууц үгийг олж авах, байнгын харилцаатай итгэмжит хамтрагч болон гэр бүл, найз нөхдөөс нь хандаж буй мэтээр банкны гүйлгээ хийлгэх зэргээр санхүүгийн хохирол төдийгүй эмзэг нууц мэдээллийг задруулах эрсдэлүүдийг учруулдаг. Сүүлийн үед хиймэл оюун ухааны салбар эрчимтэй хөгжиж бидний амьдралд томоохон ахиц дэвшлийг авчрах технологиуд ар араасаа гарч байгаа хэдий ч үүнийг буруугаар ашиглаж ашиг хонжоо олох, бусдын нэр хүндийг унагах, цахим халдлагын технологийг улам боловсронгуй боломжийг мөн давхар олгож байна. Тухайлбал, хиймэл оюун ухааны deepfake технологийг сошиал инженерчлэлийн халдлагыг улам боловсронгуй болгох зорилгоор хүний дуу хоолой, зураг, бичлэгийг машин сургалтын аргаар үүсгэж, хэн

нэгний хэлээгүй үгийг хэлсэн мэт, хийгээгүй үйлдлийг хийсэн мэт хуурамчаар үүсгэх боломжтой болж байна. Иймд энэ төрлийн халдлагаас сэргийлэхийн тулд мэдээллийн эх сурвалжийг давхар баталгаажуулах, гярхай байх хэрэгцээ шаардлага бидний өмнө тулгараад байна. Сошиал инженерчлэлийн халдлага нь дараах шинжүүдийг агуулсан байдаг. Үүнд:

- 📞 **Хүн хоорондын харилцаан дээр тулгуурлана** 👨‍💭**:** Программ хангамж, цахим төхөөрөмжүүд рүү шууд халдлага хийхгүйгээр хүнийг хууран мэхэлж, итгэлийг нь олохдоо тэдний сэтгэл зүй, айдас, шунал, тусламж хүссэн байдал дээр тулгуурлана.
- 🌐 **Итгэмжит албан байгууллага, хувь хүн мэт дүр эсгэх** 🎭 **:** Сошиал инженерчлэлийн халдлага үйлдэгч нь өөрийгөө ямар нэгэн харилцагч байгууллагын ажилтан, цагдаа, банкны ажилтан эсвэл таны нэгэн танил, найз нөхөд мэтээр дүр эсгэн танаас нэг удаагийн баталгаажуулалтын код, нэвтрэх нэр, нууц үг, асуух эсвэл банкны гүйлгээ, худалдан авалт хийх ёстой зэргээр хууран мэхэлдэг.
- 📋 **Мэдээлэл цуглуулах** 📁**:** Халдага үйлдэгч нь бай болох хүмүүсийнхээ талаарх хамт ажилладаг хүмүүсийн нэр, харилцан ярианых нь хэв маяг, үг хэллэг, хийдэг ажил бизнесийн мэдээлэл зэргийг нь цуглуулж хууран мэхлэлтээ илүү итгэхүйц бодит болгох зорилготой байдаг. Эдгээр мэдээллийг таны сошиал хуудас, веб сайт эсвэл шууд тантай харилцан ярих үедээ ч олж авах боломжтой юм.
- 😐 **Хүний сэтгэл зүйд нөлөөлөх** 😳: Халдагч этгээд нь өөрийн зорилгодоо хүрэхийн тулд бай болсон хүнийхээ эрх мэдэл, ашиг сонирхол, тусламж шаардлагатай байгаа зэрэг хэрэгцээг ашиглан түүний айдас, сэтгэл хөдлөл дээр тулгуурлан зорилгодоо хүрдэг.
- 🔐 **Яаралтай богино хугацаанд хийх шаардлагатай гэж сандаргах** 🔑: Сошиал инженерчлэлийн халдлага үйлдэгч нь тухайн халдлагад өртөж буй хүнээс түргэн хугацаанд яаралтай шийдэх эсвэл боломжийг алдахаас эмээх сэтгэгдэл төрүүлэх байдлаар тухайн хүнийг халдлагад өртөж байгааг аль болох мэдэгдэхгүйгээр яаралтай байдал үүсгэж, түүнийгээ давуу талтай болгон ашигладаг.
- 🎯 **Халдлагын бай болж байгаа хүндээ тааруулж бэлтгэгдсэн байх** 🏹: Халдагч этгээд нь бай болгож буй хүнийхээ талаар цуглуулсан мэдээлэлдээ үндэслэн итгэл төрөхүйц байхаар төлөвлөж халдлагаа хийх нь халдлагыг амжилттай болгох гол үндэс байдаг. Жишээ нь, таны өдөр тутамдаа хэрэглэдэг онлайн дэлгүүрийн хаягаас тань рүү хүргэлтийн урьдчилгаа мөнгөө шилжүүлнэ үү гэх мэтээр тухайн хүний хэрэглэдэг, мэддэг зүйлийг оролцуулах нь халдлага илүү амжилттай болох боломжийг нэмэгдүүлнэ.

Хамрах хугацаа:	**2024 оны 2-р сарын сүүлийн хагас (#2)**
Хамрах сэдэв:	**Сошиал инженерчлэлийн халдлагын төрлүүд болон тэдгээрийг таних нь**

📌 **Сошиал инженерчлэлийн халдлагын тактик болон төрлүүдийг таньж, тэдгээрээс сэргийлэх зөвлөмж**

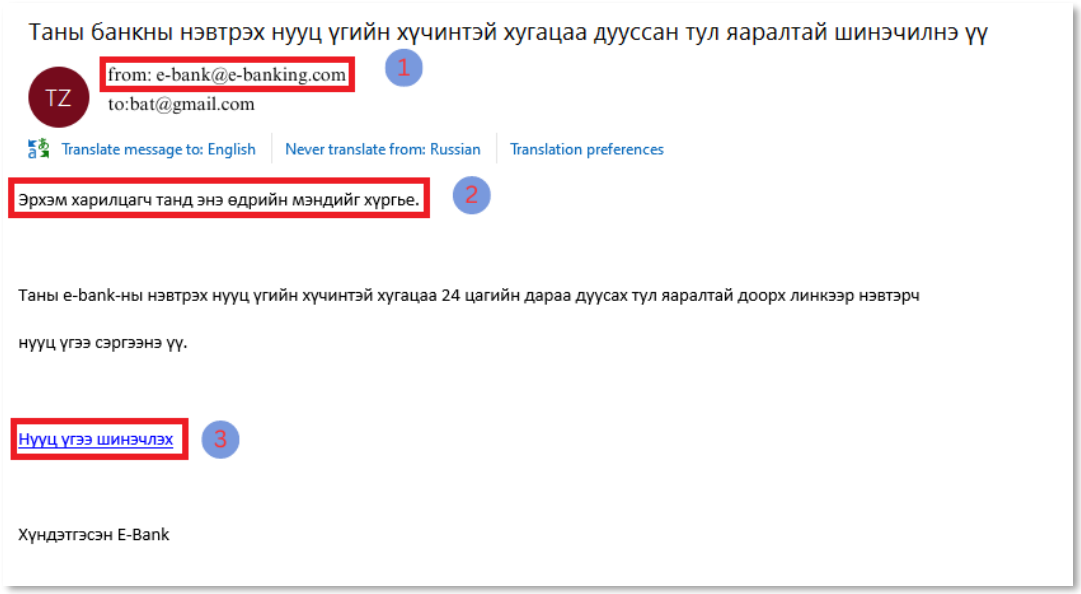
- **И-мэйл фишинг :** Сошиал инженерчлэлийн халдлагын хамгийн түгээмэл ашиглагддаг суваг болох и-мэйл фишинг нь хүлээн авагчдад итгэл төрүүлэхийн тулд итгэмжлэгдсэн эх сурвалжийн дүр эсгэсэн, хуурамч и-мэйлийг ашигладаг. Түгээмэл арга техникүүд нь и-мэйлээр албан ёсны веб хуудаснуудыг дуурайлган хийж нэвтрэх нэр, нууц үгийг хулгайлах, хортой файл хавсралтаар илгээх байдаг. Халдлага үйлдэгчид и-мэйл фишинг халдлагыг өргөн цар хүрээтэйгээр явуулахад хэлний бэрхшээл тулгардгаас болж хэт их үг үсэг, утга зүйн алдаа гаргадаг байсан нь фишинг халдлагыг таньж, илрүүлэх нэгэн томоохон шинж тэмдэг байсан. Гэтэл одоо үед орчуулгын программ хангамжууд улам боловсронгуй болж байгаа нь уг төрлийн халдлагыг таньж, илрүүлэхэд илүү төвөгтэй болгосоор байна. И-мэйл фишинг төрлийн халдлагаас сэргийлэхийн тулд и-мэйлийн илгээгчийн хаяг үнэн зөв байгаа эсэх, үг үсэг, утга зүйн алдаа их байгаа эсэх, илгээсэн линк нь албан ёсны вебийн домэйнтэй таарч байгаа эсэхийг нягтлахаас гадна илгээсэн хавсралт файлыг анти-вирусийн программаар шалгаж хортой эсэхийг нягтлах алхмуудыг хэрэгжүүлэх хэрэгтэй.

- **Вишинг : И-мэйл фишинг төрлийн халдлагатай адилхан боловч ашиглаж буй харилцаа холбооны хэрэгсэл нь утасны дуудлага юм. Ихэвчлэн банкны ажилтан, таны харилцдаг ямар нэгэн албан ёсны байгууллагын ажилтан тантай холбоо барихаар ярьж буй мэт дүр эсгэн нэвтрэх нэр, нууц үг, кодыг асууж мэдэх эсвэл банкны гүйлгээ хийлгэх зэргээр эрсдэл учруулдаг. Хиймэл оюун ухааны тусламжтай deepfake технологиор бусдын дуу хоолойг дуурайх боломж бий болсон тул танихгүй дугаарын ард таны бизнесийн хамтрагч, танил нэгний тань дуу хоолойг нь дуурайлган тоглуулсан robocall ч байх эрсдэлтэй. Тань руу хэн нэгэн утсаар залгаж нууцлалтай мэдээлэл асууж байгаа тохиолдолд эх сурвалжийг үнэн зөв эсэхийг тодруулах, нэвтрэх эрхийн мэдээлэл, утсанд ирсэн кодыг өгөхгүй байх дээр анхаарах нь вишинг халдлагаас сэргийлэх үндсэн арга зам юм.

- 🤷 **Өгөөш** ⁉️: Хүний сониуч зангаас үүдэж хэн нэгнээс авсан, олсон өгөөш буюу хор хөнөөлтэй зорилго бүхий USB флаш диск, зөөврийн төхөөрөмжүүдийг байгууллагын болон хувийн төхөөрөмжүүд рүүгээ залгаснаар түүнд агуулагдаж буй хортой кодод өртөж мэдээллээ алдах эрсдэлтэй байдаг. Хүнээс авсан болон хаа нэгтэйгээс олсон зөөврийн төхөөрөмжүүдийг хувийн болон байгууллагын компьютерт шууд залгахгүй байх, тэдгээр төхөөрөмжийг зайлшгүй ашиглах шаардлагатай тохиолдолд ашиглахын өмнө анти-вирусийн программаар скан хийж шалгах шаардлагатай.
- 🦹 **Хуурамч мэдээлэл өгөх** ❓: Энэ нь бусдад өөрийгөө гаднын зөвлөх ажилтан, аудитор, шинжээч гэх мэтээр худал мэдээлэл өгч танилцуулан байгууллагын ажилтан болон хувь хүнээс нууцлалтай мэдээллийг нь олж авах зорилготойгоор хийддэг халдага юм. Байгууллага болон хувь хүний нууцтай мэдээллийг өөрийгөө баталгаажуулаагүй аливаа гаднын этгээд, хувь хүнд өгөхгүй байх нь энэ төрлийн халдлагын хохирогч болохоос сэргийлнэ.
- 💵 **Ашиг хонжоон дээр суурилсан буюу Quid pro quo халдлага** 💲**:** Энэ төрлийн тактик нь хамгийн түгээмэл байдаг бөгөөд ямар нэгэн байгууллагын хямдрал урамшууллыг хуурамчаар үүсгэн тараах замаар хохирогчдоос нэвтрэх нэр, нууц үг болон бусад халдагын зорилгод шаардлагатай мэдээллийг цуглуулах хэлбэрээр явагддаг. Хямдрал, уралдаан зарласан эх сурвалжийн үнэн зөвийг баталгаажуулахгүйгээр хувийн мэдээллээ өгөхгүй байх нь энэ төрлийн халдлагаас урьдчилан сэргийлэх арга зам юм.
- 🔒 **Физик орон зайд бодитоор үйлдэгдэх tailgating халдлага** 🏦**:** Энэ төрлийн халдлага нь нэвтрэх хязгаарлалт бүхий барилга, байгууламж руу зөвшөөрөлгүй нэвтрэх эрхийг хуурамчаар үйлдэх, бусдыг хуурч залилан дагаж орох эсвэл шалган нэвтрүүлэлтийн алдаатай процессыг ашиглаж нэвтрэх зэргээр хийгддэг. Энэ төрлийн халдлагаас сэргийлэхийн тулд барилга, байгууламж руу нэвтэрч буй аливаа гаднын хүний өгсөн мэдээлэл үнэн зөв эсэхийг баталгаажуулах, хязгаарлалтай бүс рүү нэвтрэх процесс нь журмын дагуу алдаагүй явагдаж байгаа эсэх дээр анхаарах шаардлагатай юм.

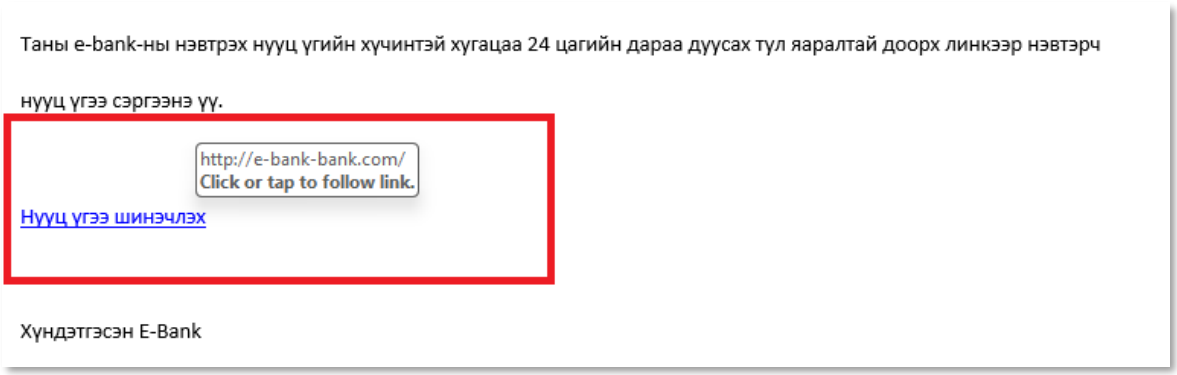
СОШИАЛ ИНЖЕНЕРЧЛЭЛИЙН ХАЛДЛАГЫГ ТАНИХ ЖИШЭЭ ЗААВАР

📌 Сошиал инженерчлэлийн хадлагын хамгийн түгээмэл арга болох фишинг и-мэйлийн жишээг ***Зураг 1***-д харуулсан зургаас авч үзье. Таны ашигладаг банкийг **e-bank.mn** гэж байсан үзвэл танд банкнаас ирэх и-мэйлийн **from:** буюу илгээгчийн хаяг нь **@e-bank.mn** байх ёстой. Гэвч ***Зураг 1***-ийн 1 дугаартай хэсэгт харуулсанчлан илгээгчийн хаяг нь **@e-banking.com** гэсэн байгаа нь банкны албан ёсны хаягаас биш байгаа нь фишинг халдлага болохыг илтгэж байгаа нэг шинж тэмдэг юм.



Зураг 1. Фишинг и-мэйлийн жишээ

И-мэйлийн ***Зураг 1***-ийн 2 дугаартай хэсэгт харуулсан агуулгын тухайд хэрвээ албан байгууллага нь хэрэглэгчид рүүгээ и-мэйл илгээхдээ ихэвчлэн тухайн хэрэглэгчийн нэрийг оруулсан мэндчилгээ хүргэдэг. Энэ тохиолдолд ерөнхий мэндчилгээ ашигласан байгаа нь сэжигтэй гэж үзэх нэг шинж болж байна. ***Зураг 2***-т харуулсан нууц үгээ шинэчлэх хэсэгт компьютерын хулганаа даралгүйгээр холбоос дээр байрлуулахад хандах гэж буй линк нь доорх зурган дээрх шиг харагддаг. Энэ тохиолдолд мөн **e-bank.mn** гэсэн албан ёсны домэйн хаяг нь биш **e-bank-bank.com** гэсэн байгаа нь фишинг халдлага буюу таны банкны нэвтрэх нэр, нууц үгийг авах оролдлого гэдгийг баталж байгаа юм.



Зураг 2. Фишинг и-мэйлийн жишээ

📌 Сошиал инженерчлэлийн халдлагын дараагийн жишээ болгон тань руу утсаар холбогдож танаас нууцлалтай мэдээллийг олж авах зорилготой вишинг халдлагыг авч үзье.

E-bank-ыг ашигладаг Баттай e-bank-ны харилцагчийн үйлчилгээнээс холбогдож байна гэж нэгэн өдөр утсаар холбогдов. Холбогдсон хүн нь үнэндээ банкны ажилтан биш түүний интернэт банкны эрхийг олж авах гэсэн халдагч байв.

Халдагч: “Сайн байна уу? Тантай e-bank-ны харилцагчийн үйлчилгээний хэсгээс холбогдож байна.”
Бат: “Сайн, сайн байна уу?”
Халдагч: “Таны интернэт банкны хэрэглэгчийн мэдээллийг шинэчлэх хугацаа болсон байна. Мэдээллийн шинэчлэлтийг 24 цагийн дотор өөрийн биеэр банкны салбар дээр ирж өгөх эсвэл одоо хамт утсаар өгөөд хийх боломжтой байна.”
Бат: “Өө тийм үү. Надад банк орох зав байхгүй. Одоо утсаар өгчихвөл удах уу?”
Халдагч: “Тэгвэл танд мэдээллээ шинэчлэх 4 оронтой кодыг утас руу тань мессежээр илгээлээ. Илгээсэн кодыг хэлээрэй.”
Бат: “2231 гэж байна.”
Халдагч: “За таны мэдээлэл шинэчлэлтийг эхлүүлье. Таны оршин суугаа хаяг өөрчлөгдсөн байгаа юу?”
Бат: “Үгүй, хэвээрээ байгаа.”
Халдагч: “Яаралтай үед холбоо барих нэмэлт нэг дугаар?”
Бат: “99123412”
Халдагч: “За та дараа өөрт ойрхон байрлах банкны аль нэг салбарт очоод иргэний үнэмлэхийн хуулбараа дахин өгөөрэй. Танд баярлалаа.”
Бат: “За ойлголоо, баярлалаа.”

Дээрх жишээнээс харахад Батад банкнаас үйлчилгээ санал болгосон иймэрхүү дуудлагууд үе үе ирдэг байсан тул нэг их зүйл бодолгүй мессежээр ирсэн кодыг хэлээд өгчхөв. Гэвч энэ нь банкны ажилтан биш байсан бөгөөд түүний утасны дугаараар нь код авч, түүний банкны нэвтрэх эрхийн нууц үгийг нь шинэчилж орох гэсэн халдага үйлдэгч байсан гэдгийг цахим халдлагын талаар мэдлэг, мэдээлэл дутмаг тэрээр мэдэлгүй өгч вишинг төрлийн халдлагын хохирогч болсон байв.

Дээрх тохиолдлоос харвал Бат нь банкны ажилтан хэзээ ч хэрэглэгчээсээ нэвтрэх нэр, нууц үг, код асуудаггүй, мөн хэрэглэгчийн тухай мэдээллийг утсаар болон и-мэйлээр авах ёсгүй гэдгийг тэрээр мэддэггүй байсан тул халдлагын хохирогч болж байна. Иймд ямар нэгэн баталгаагүй эх сурвалжаас таны нууцлалтай мэдээллийг асуусан төрөл бүрийн дуудлага, мессеж, чатад нэр, нууц үг, кодыг хэлж болохгүйг анхааараарай.

ДҮГНЭЛТ

Сошиал инженерчлэл нь цахим хэрэглээ хурдацтайгаар өсөн нэмэгдэж байгаа өнөө үед хамгийн түгээмэл халдлагын төрөл болоод байна. Учир нь энэ төрлийн халдлага нь нарийн төвөгтэй цахим аюулгүй байдлын хамгаалалтуудыг нэвтэрч программ хангамж, сүлжээ рүү чиглэж халдлага үйлдэхээс илүү хувь хүн, албан байгууллагын ажилтны цахим аюулгүй байдлын мэдлэг дутуу, анзааргүй байдал дээр тулгуурлаж халдлагаа үйлдэх нь халдагч нарт хялбараар зорилгодоо хүрэх боломжийг бүрдүүлж байгаа тул сошиал

инженерчлэлийн халдлагын төрөл, түүний шинж чанар, хэрхэн таньж эрсдэлээс урьдчилан сэргийлэх талаар мэдээллийг та бүхэнд энэхүү сэдвээрээ хүргэлээ.

ОЙЛГОЛТ ШАЛГАХ АСУУЛТУУД

1. Сошиал инженерчлэл гэж юу вэ? Хамгийн оновчтой нэг хариултыг сонгоно уу.
   a. Сошиал харилцаа холбоо үүсгэх
   b. Хүмүүсийг хуурч мэхлэн эмзэг нууцлалтай мэдээллийг олж авах зорилготой үйлдэл
   c. Сошиал платформыг сайжруулах инженерчлэлийн арга
   d. Нийгмийн харилцааг зохицуулах инженерчлэл
2. Аль нь сошиал инженерчлэлийн халдлагын төрөл вэ?
   a. Фишинг
   b. Эмзэг байдалтай программ хангамж
   c. Сүлжээний буруу тохиргоо
   d. Цахим хамгаалалтын системийг давах
3. Аль сонголт нь сошиал инженерчлэлийн вишинг халдлагыг илэрхийлж байна вэ?
   a. И-мэйлээр хортой код илгээх
   b. Утасны дуудлага, дуут мессежээр нууцлалтай мэдээлэл асуух
   c. Нэвтрэх хязгаарлалт бүхий байгууллага руу хуурамч мэдээллээр нэвтрэх
   d. Компьютерт хортой программ суулгах
4. Сошиал инженерчлэлийн халдлагаас сэргийлэх хамгийн зөв алхам юу вэ?
   a. Хүчтэй нууц үг ашиглах
   b. Нууцлалтай мэдээллийг эх сурвалжийг нь баталгаажуулахгүйгээр өгөхгүй байх
   c. Анти-вирусийн программ хангамж ашиглах
   d. Ирсэн и-мэйлийн линкээр орж баталгаажуулах
5. Хортой кодтой USB флаш диск компьютерт залгах арга барилыг ашигладаг сошиал инженерчлэлийн халдлага аль нь вэ?
   a. Фишинг
   b. Вишинг
   c. Өгөөш
   d. Quid pro qui