

1. НУУЦ ҮГ

- Интернет банкны нууц үгээ сонгохдоо тоо, үсэг, тэмдэгт зэргээс бүрдсэн нууц үг ашиглах;
- Интернет банк ашиглаж гүйлгээ хийх, дансны үлдэгдлээ шалгахдаа цаасаар хэвлэхгүй, цаас ашиглахгүй байх, вэб хөтөч дээрээ автоматаар сануулж хадгалахгүй байх;
- Интернет банкны нэр, нууц үг, картын дугаар, хүчинтэй хугацаа, CVV дугаар, PIN дугаар зэрэг нууц мэдээллээ и-мэйлээр дамжуулахгүй байх;
- Та интернет банкны үйлчилгээнд ашигладаг нууц үгээ тодорхой давтамжтайгаар сольж байх хэрэгтэй. Жишээлбэл: 1-2 сар тутам эсвэл улирал тутамд сольж байхыг зөвлөж байна.

2. ИНТЕРНЕТ БАНК

- Хэрэглэгчийн нэр, дансны дугаар болон нууц үгээ бусдад задруулахгүй байх;
- Интернет банкаар гүйлгээ хийхдээ хүлээн авагчийн болон бусад мэдээллийг үнэн зөв оруулсан эсэхийг шалгах;
- Интернет банкаар хийгдсэн гүйлгээний баримт, хариу мессежийг тогтмол шалгаж хэвших, энэ нь ямар нэгэн сэжигтэй гүйлгээ таны нэр дээр хийгдсэн эсэхийг илрүүлэх ач холбогдолтой;
- Таны бүртгэлийн мэдээлэл (Утасны дугаар, и-мэйл хаяг, оршин суугаа хаяг) өөрчлөгдсөн тохиолдолд өөрт ойр байрлах Тээвэр хөгжлийн банкны салбарт хандан мэдээллээ шинэчилж хэвших;
- Хэрэв та өөрийн дансанд ямар нэгэн сэжигтэй гүйлгээ хийгдсэнийг илрүүлбэл нэн даруй Тээвэр хөгжлийн банкны Лавлах төвийн 7716-9999 дугаарт холбогдон мэдэгдэх;

3. НЭВТРЭХ ПРОЦЕСС

- Интернет банкны үйлчилгээг нийтийн хэрэглээний компьютероос авахыг аль болох татгалзах зайлшгүй авсан тохиолдолд;
- Интернетийн орчинд цахим банк ашигласан бол гарах товчийг дарах буюу log out хийж хэвших;
- Ашигласан программуудаа хаах;
- Дансны хуулга зэрэг хувийн мэдээллээ үлдээхгүй байх;
- Та хэрэв илүү баталгаа хүсвэл нийтийн компьютер ашигласны дараа аюулгүй газраас нууц үгээ солих;

4. КОМПЬЮТЕР БОЛОН МОБАЙЛ

- Вирусийн болон бусад хор хөнөөлтэй програмаас сэргийлсэн төхөөрөмж, програм хангамжуудыг заавал ашиглах;
- Үйлдлийн систем, хэрэглээний програм хангамж, браузерууд болон интернет банкны смарт аппликейшны сүүлийн хувилбар, сайжруулалтыг тогтмол суулгах;

5. СҮЛЖЭЭ

- Утасгүй сүлжээг ашиглаагүй үед функцуудыг хаалттай байлгах (Wireless, Bluetooth, NFC гэх мэт);
- Нийтийн хэрэглээний, хамгаалалтгүй, үнэгүй утасгүй сүлжээ ашиглахдаа мэдээлэл алдах эрсдэлтэй болохыг анхаарах;

6. ХУДАЛДАН АВАЛТ:

- Таны ашиглаж буй вебсайт нь SSL-ээр (https://) баталгаажсан эсэхийг шалгаарай, ийм вэб сайтууд нь таны гүйлгээний мэдээллийг нууцалдаг.
- Таны хийсэн гүйлгээний хуулга сарын сүүлээр ирэхийг хүлээлгүй дансаа тогтмол шалгаж байгаарай, баталгаатай олон нийтэд хүлээн зөвшөөрөгдсөн вэб сайтаар гүйлгээ хийсэн ч шалгаж байх;
- Интернет кафе зэрэг олон хийт ашигладаг компьютер ашиглан интернет худалдан авалт хийхгүй байхыг анхаарах; Тухайн компьютер дээр онлайн худалдан авалт хийхэд оруулсан мэдээллүүд хадгалагддаг, мөн санаандгүй log out хийлгүй гарсан тохиолдолд таны дансанд өөр хэн нэгэн хандах бүрэн боломжтойг анхаарах;
- Олон нийтийн Wi-Fi сүлжээнд холбогдсон үедээ онлайн худалдан авалт хийхээс татгалзаарай. Учир нь таны бүх мэдээлэлд Wi-Fi цацаж буй этгээд хандах боломжтой байдаг.

ХЭРХЭН ХУУРАМЧ И-МЭЙЛЭЭС СЭРЭМЖЛЭХ ВЭ?

Интернет банкны харилцагч танд цахим ертөнцийн халдлагуудын нэг болох Фишинг /Phishing/ халдлагаас хэрхэн сэргийлэх талаар мэдээлэл хүргэж байна.

ФИШИНГ ХАЛДЛАГА ГЭЖ ЮУ ВЭ?

Хакерууд таны төлбөрийн карт болон интернет банкны нууцлалын талаар мэдээлэл авах зорилгоор хуурамч и-мэйл илгээдэг.

Хуурамч и-мэйлийг хэрхэн таних вэ?

- Банк хэрэглэгчидрүү дансны мэдээллээ онлайнгаар өөрчлөх, шинэчлэх, нууц мэдээллээ илгээхийг хүссэн и-мэйл илгээдэггүй. Танд ийм утгатай и-мэйл ирсэн тохиолдолд итгэж болохгүйг анхаарах;
- Та хулганаа холбоос дээр аваачихад тэрхүү холбоосны цаанаас жинхэнэ URL хаяг харагдах болно. Хэрэв тэрхүү хаяг нь банкны жинхэнэ холбоосноос өөр, сэжигтэй харагдаж байвал тэрхүү и-мэйл хуурамч болохыг анхаарах;