ЦАХИМ ОРЧИН ДАХЬ ОЛОН НИЙТИЙН СҮЛЖЭЭ (FACEBOOK)-НИЙ АЮУЛГҮЙ БАЙДАЛ

1. Цахим бүртгэлээ хамгаалах

1.1. Хүчирхэг нууц үг үүсгэх, нууц үгээ хамгаалах

1.2. Нэвтрэх мэдээллээ хуваалцахгүй байх

1.3. Танихгүй хүний найзын хүсэлтийг зөвшөөрөхгүй байх

2. Спам болон луйвраас зайлсхийх

2.1. Луйвраас зайлсхийх

2.2. Фишинг халдлагаас хамгаалах

2.3. Нийтлэг луйврууд

2.4. Сэжигтэй имэйл, мессежийг таних

3. Хортой программ хангамж

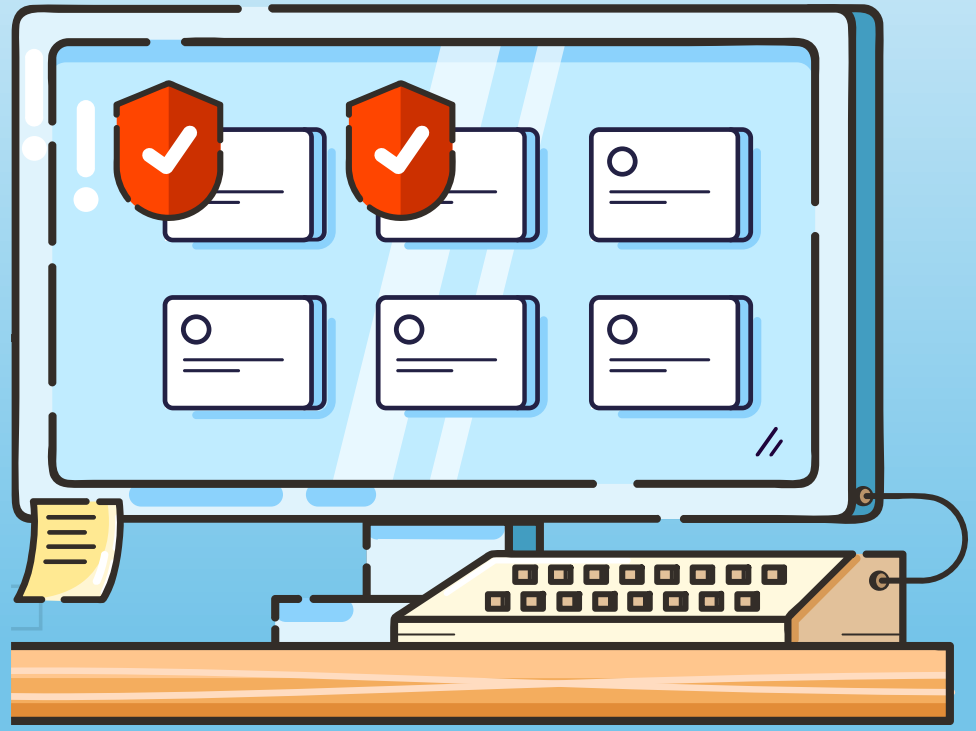
4. Холбоос аюулгүй эсэхийг шалгах

5. Аюулгүй байдлын зөвлөмжүүд

6. Сэрэмжлүүлэг болон хоёр нөхцөлт танилт (Two-factor authentication)-ын тохиргоог идэвхжүүлэх

6.1. Сэрэмжлүүлэг илгээх тохиргоог идэвхжүүлэх

6.2. Two-factor authentication тохиргоог удирдах



Хүчирхэг нууц үг (Strong password) үүсгэх

- Нууц үг урт байх тусам илүү найдвартай байдаг. Өөр хэн ч мэдэхгүй үг хэллэг эсвэл хэд хэдэн үг ашиглан урт болгох.
- Том, жижиг үсэг, цифр, тэмдэгтийг хольж оруулах зэргээр илүү найдвартай болгох боломжтой.
- Таны нууц үгийг таахад хэцүү байлгахын тулд нийтлэг үг бүү ашиглаарай. “password“, “12345678” гэх мэт нийтлэг үгсийг ашигласнаар та өөрийгөө аюулд оруулна.
- Таны нууц үг таны нэр, имэйл, утасны дугаар, төрсөн өдөр гэх мэт мэдээллийг агуулаагүй байх.

Нууц үгээ хамгаалах

- Таны Фэйсбүүк бүртгэлд ашиглаж буй нууц үг таны цахим шуудан, цахим банк гэх мэт бусад систем рүү нэвтрэхэд ашигладаг нууц үгээс өөр байх.
- Нууц үгээ бусадтай хуваалцахгүй байх. Хэрэв мэдэгдсэн тохиолдолд нууц үгээ нэн даруй өөрчлөх.
- Шаардлагатай гэж үзвэл таны нууц үгийг найдвартай хадгалах олон төрлийн нууц үгийн менежментийн аппликэйшнүүдээс ашиглах. Жишээ нь, NordPass, 1Password.

Нэвтрэх мэдээллээ хуваалцахгүй байх

- Луйварчид Фэйсбүүктэй төстэй хуурамч вэбсайт/аппликэйшн үүсгэж, цахим шуудан, нууц үгээрээ нэвтэрч орох хүсэлт ирүүлэх боломжтой.
- Вэб хөтчөөр Фэйсбүүкт нэвтэрч буй тохиолдолд нэвтрэх мэдээллээ оруулахаас өмнө URL-г шалгах. Хэрэв эргэлзэж байвал хөтөч дээрээ www.facebook.com гэж бичээд Фэйсбүүкт нэвтрэх.
- Метагаас ирүүлсэн и-мэйл нь таны Фэйсбүүк бүртгэлийн нууц мэдээллийг агуулсан байж болзошгүй тул бусад хүмүүст илгээхгүй байх. Мөн бусадтай хуваах хэрэглэдэг компьютер, гар утсан дээрх Фэйсбүүк бүртгэлээс гарч байх.

Танихгүй хүний найзын хүсэлтийг зөвшөөрөхгүй байх

- Луйварчид хуурамч бүртгэл үүсгэж найзын тоогоо нэмэхийг оролддог.
- Луйварчидтай найз болох нь тэдэнд таны мэдээллийг ашиглан хуурамч нийтлэл оруулах, таныг нийтлэлд тэмдэглэх, танд хортой мессеж илгээх боломжийг олгоно.

Найзын хүсэлтийг хүлээн авах эсвэл мессежинд хариу өгөхдөө дараах шинж тэмдгүүдийг анхаараарай. Үүнд:

- Мөнгө гуйж байгаа танихгүй эсвэл алдартай хүмүүс
- Зээл, шагнал эсвэл бусад хожлыг танд өгөхийн тулд урьдчилгаа хураамж авахыг хүсч байгаа
- Найз нөхөд, хамаатан садны хүмүүсээс ирж буй яаралтай мессеж
- Таныг өөр платформ дээр харилцахыг хүсэх/урих
- Хайр дурлалын харилцаа тогтоож мөнгө нэхэх
- Үг үсгийн алдаа, дүрмийн алдаатай нийтлэл, мессеж
- Таны цахим бүртгэлд алдаа байгаа тул яаралтай хариу өгөхийг хүссэн утгатай мессеж
- Таны ашигладаг үйлчилгээний мэдэгдэл ирж таниас нийгмийн сүлжээ, имэйл, банкны дансаараа нэвтрэхийг хүссэн мессеж
- Фэйсбүүк дээр найзгүй, нүүр зураггүй, идэвхгүй хаягаас найзын хүсэлт ирэх

Луйвраас зайлсхийх

- Хурдан бөгөөд хялбар хөрөнгө оруулалтын схемийг санал болгосон мэйл,
- Тусламж хэрэгтэй байгаа Фэйсбүүк дэх найзын яаралтай мессеж,
- Метагаас ирсэн гэх бөгөөд таны бүртгэлтэй холбоотой асуудлын талаар анхааруулж, яаралтай хариу хүссэн фишинг и-мэйл зэргээс болгоомжлох
- Тэд таны болон таны найзуудын мөнгө, хувийн мэдээллийг залилан мэхлэхийн тулд бусдын дүр эсгэх, эсвэл таны бүртгэлийг хакердэж, хуурамч бүртгэл үүсгэж болзошгүй.

Фишинг халдлагаас өөрийгөө хамгаалах

Фишинг гэдэг нь хэн нэгэн таны хувийн мэдээллийг авахыг хүссэн сэжигтэй мессеж эсвэл холбоос илгээж таны бүртгэл рүү нэвтрэх оролдлого юм. Хэрэв тэд таны бүртгэлд нэвтэрвэл спам илгээхдээ таны бүртгэлийг ашиглаж болзошгүй.

Фишинг и-мэйл нь дараах агуулгатай ирдэг. Жишээ нь:

- “Чухал мэдэгдэл ирлээ, тухайн мессежийг уншихын тулд Фэйсбүүк бүртгэл рүүгээ нэвтрэх шаардлагатай”.
- Тус имэйл нь Фэйсбүүк рүү биш хуурамч, албан бус холбоост нэвтрэхийг зааварчлах бөгөөд холбоос дээр дарахад хэрэглэгчийн нэр, нууц үгээ оруулахыг шаарддаг.

Нийтлэг луйвар

- Хөрөнгө оруулалтын луйвар: Бага хэмжээний мөнгийг илүү их мөнгө болгон хөрвүүлэхийг санал болгох, бодит бус мөнгөний ашгийг амлаж болно. Ихээхэн ашиглагддаг хөрөнгө оруулалтын луйврууд нь **cash flipping** луйвар, **Ponzi** схем, **get rich quick** схемүүд юм.

- Хайр дурлалын луйвар: Салсан, бэлэвсэрсэн, муу гэр бүлтэй болсон мэт дүр эсгэж, харилцаа тогтоон романтик мессеж илгээдэг. Нислэг худалдаж авах, виз мэдүүлэхэд мөнгө эсвэл таны мэдээлэл хэрэгтэй гэж хэлдэг. Тэдний зорилго нь эхлээд таны итгэлийг олж авах явдал учраас мөнгө гуйхаасаа өмнө хэдэн долоо хоног, сараар яриа өрнүүлж харилцаа тогтоож болзошгүй.

- Ажлын байрны луйвар: Луйварчид төөрөгдүүлсэн хуурамч ажлын зарыг ашиглан таны хувийн мэдээлэл, мөнгийг авахыг оролддог. Хэтэрхий сайхан сонсогдож байгаа, таны өргөдлийг хэлэлцэхээс өмнө урьдчилгаа төлбөр төлөхийг шаарддаг ажлын зараас зайлсхийх хэрэгтэй. Ажлын зарын холбоос дээр дарахад ажлын зартай холбоогүй эсвэл таны нууц мэдээллийг авахыг хүссэн вэбсайтаас болгоомжлох.

- **Сугалааны залилан:** Луйварчид албан ёсны байгууллагын дүрд хувирч таныг бага хэмжээний урьдчилгаа төлбөр төлөөд авах боломжтой сугалааны цорын ганц азтан болсон гэж мэдэгдэнэ. Мөн таныг азтан мөн эсэхийг баталгаажуулах зорилгоор таны хаяг, банкны дэлгэрэнгүй мэдээлэл гэх мэт хувийн мэдээллээ өгөхийг хүснэ.
- **Зээлийн луйвар:** Луйварчид бага хэмжээний урьдчилгаа төлбөр төлөөд бага хүүтэй шуурхай зээл санал болгох мессеж эсвэл сэтгэгдэл үлдээдэг. Урьдчилгаа төлбөрийг шилжүүлсний дараа тэд илүү их зээл олгохын тулд илүү их мөнгө нэхэх эсвэл зүгээр л алга болно.
- **Хандивын луйвар:** Луйварчид буяны байгууллага, асрамжийн газар, шашны зүтгэлтнийг төлөөлж буй мэт дүр эсгэн хандив гуйх тохиолдол байдаг.
- **Өв залгамжлах луйвар:** Луйварчид нас барсан хүний үл хөдлөх хөрөнгийн өв залгамжлалтай холбоотой хандаж буй хуульч гэж мэдэгддэг. Тэд таныг өв залгамжлах эрхтэй гэж мэдэгдэж, энэхүү өвийг залгамжилж авахын тулд өөрийн хаяг, банкны дэлгэрэнгүй мэдээлэл гэх мэт хувийн мэдээллээ өгөхийг хүсдэг.

- **Худалдааны луйвар:** Луйварчид онлайнаар бараа, үйлчилгээ худалддаг гэж мэдэгдэнэ. Та тэдэнд мөнгө төлсний дараа тэд хариу өгөхөө болино.
- **Төлбөртэй үйлчилгээ** (subscription services): Луйварчид насан туршийн хугацаатай төлбөрт цахим үйлчилгээг нэг удаагийн төлбөрөөр худалдаж авахыг санал болгоно.

Сэжигтэй и-мэйл эсвэл мессежийг таних

Сэжигтэй мессеж эсвэл и-мэйлийг таньж чадвал фишинг залилангаас зайлсхийх боломжтой.

1. Дараах мессежүүдэд бүү итгээрэй. Үүнд:
    - Мөнгө гуйх
    - Бэлэг санал болгох
    - Бүртгэлийг хаана, устгана гэж сүрдүүлэх
2. Таны бүртгэлтэй холбоотой албан ёсны и-мэйлүүд зөвхөн дараах хаягаас ирдэг гэдгийг анхаараарай. Үүнд:
    - @meta.com
    - @facebook.com

Хэрэглэгч хүссэн үедээ www.facebook.com хаягаар эсвэл Фэйсбүүк аппликейшнээр нэвтэрч албан ёсны, чухал мессежүүдийг шалгаж баталгаажуулах боломжтой байдаг.

Хортой програм хангамжийн шинж тэмдэг

Хортой программ хангамж нь таны компьютер, гар утас, вэб хөтчийг (Chrome, Firefox гэх мэт) хордуулж болзошгүй.

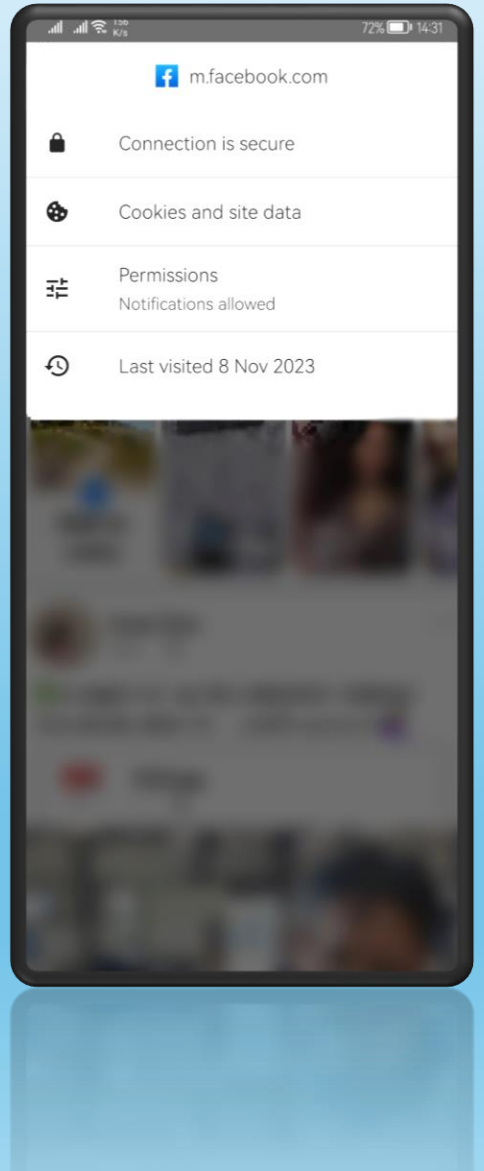
Фэйсбүүк хортой программ хангамжийн халдвар авсан байж болзошгүй шинж тэмдгүүд. Жишээ нь:

- Таны хаягаас спам эсвэл хүсээгүй мессеж илгээгдэх
- Таны бүртгэлийн түүхэнд сэжигтэй газруудын нэвтрэлт байх
- Таны үйл ажиллагааны бүртгэл (activity log)-д мэдэхгүй мессеж, нийтлэл байх

- **Компьютер эсвэл ухаалаг төхөөрөмж дээр:**
  - Таны програмууд удаан ажилладаг болох
  - Таны суулгаагүй шинэ програм суугдсан байх
  - Вэб хөтөч нээгдээгүй байхад зохисгүй зарууд гарч ирэх

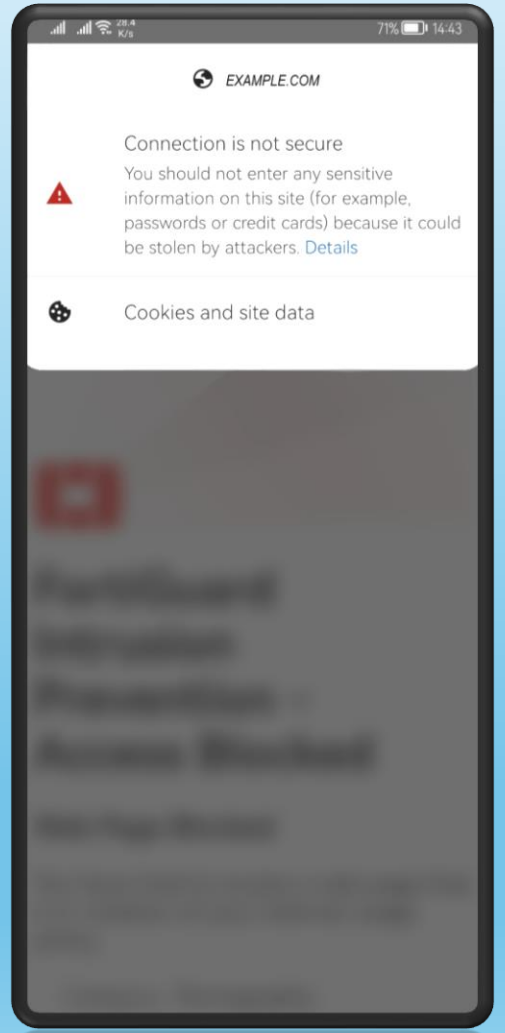
- **Таны вэб хөтөч дээр:**
  - Таны хайлтын систем эсвэл нүүр хуудас өөрчлөгдсөн байх

Хэрэв таны компьютер эсвэл ухаалаг төхөөрөмж дээр хортой программ хангамж гарч ирвэл өөрийгөө хамгаалахын тулд аль болох хурдан устгах.



Холбоос баталгаатай:

- Таны зочилж буй цахим хуудасны URL-н хажууд цоож (Connection is secure) харагдаж байвал таны ухаалаг төхөөрөмж болон тус вэбсайт хооронд аюулгүй холболттой бөгөөд Secure Socket Layer (SSL) технологиор таны оруулсан нууц үг, зээлийн картын дугаар зэрэг нууц мэдээллийг хамгаалсан, холбоос шифрлэгдсэн болохыг илэрхийлнэ.



Холбоос баталгаагүй:

- Баталгаагүй цахим хуудаст нэвтрэхэд URL-н хажууд найдваргүй холболтын анхааруулга (Connection is not secure) харагдана.
- Цахим хуудаст нэвтрэх боломжтой боловч таны төхөөрөмж болон зочилж буй вэбсайтын хооронд аюулгүй холболт байхгүй тул таны оруулсан нууц үг, зээлийн картын дугаар гэх мэт нууц мэдээлэл шифрлэгдэхгүй.

Сэжигтэй холбоос дээр бүү дараарай. Үүнд:

- Таны таньдаг хаягаас илгээсэн холбоосууд.
- Фэйсбүүк дээрх болон и-мэйлээр ирсэн бүх холбоосууд.
- Мета хэзээ ч таны нууц үгийг и-мэйлээр асуухгүй гэдгийг санаарай.
- Хэрэв танд Фэйсбүүкээс сэжигтэй и-мэйл, мессеж ирсэн бол холбоос, хавсралт дээр дарж болохгүй. Эхлээд Фэйсбүүкээс ирсэн эсэхийг сайтар шалгана уу.

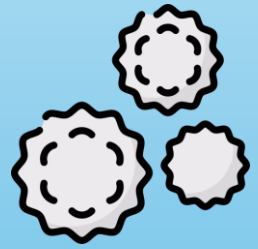
Танихгүй хүмүүсээс ирж буй файл, программ хангамжийг бүү татаарай.

- Гуравдагч талын програмуудыг суулгахдаа болгоомжтой байгаарай.
- Ялангуяа үнэн бус, хэт сайн функцуудыг санал болгодог эсвэл эхлээд бүртгэл рүү нэвтэрч орохыг шаарддаг бол анхаарах шаардлагатай.

Дараах мэдээллийг ирүүлэхийг хүссэн мессежүүдэд бүү хариулаарай:

- Нууц үг
- Нийгмийн даатгалын дугаар
- Зээлийн картын мэдээлэл

5. Аюулгүй байдлын зөвлөмжүүд



- ✓ Интернэт дэх өөрийн бүртгэлдээ аюулгүй байдлын нэмэлт хамгаалалт нэмэхийн тулд хоёр нөхцөлт танилт (Two-factor authentication)-ын тохиргоог идэвхжүүлнэ үү.
- ✓ Хоёр нөхцөлт танилт (Two-factor authentication) нь дансны нууцлалыг зөрчих оролдлоготой тэмцэх хамгийн үр дүнтэй хэрэгслүүдийн нэг юм.
- ✓ Өөр платформ дээр нууц үгээ дахин бүү ашиглаарай.
- ✓ Итгэмжлэгдсэн вирусны эсрэг программ ашиглаж болно.
- ✓ Бүртгэлгүй төхөөрөмж, хөтчөөс нэвтэрсэн тохиолдолд сэрэмжлүүлэг илгээх тохиргоог идэвхижүүлснээр хэн нэгэн таны бүртгэлд нэвтрэх оролдлого хийхэд танд мэдэгдэнэ.
- ✓ Таны бүртгэлд ямар төхөөрөмж нэвтэрснийг мэдэхийн тулд нэвтэрсэн түүхийг шалгаарай.

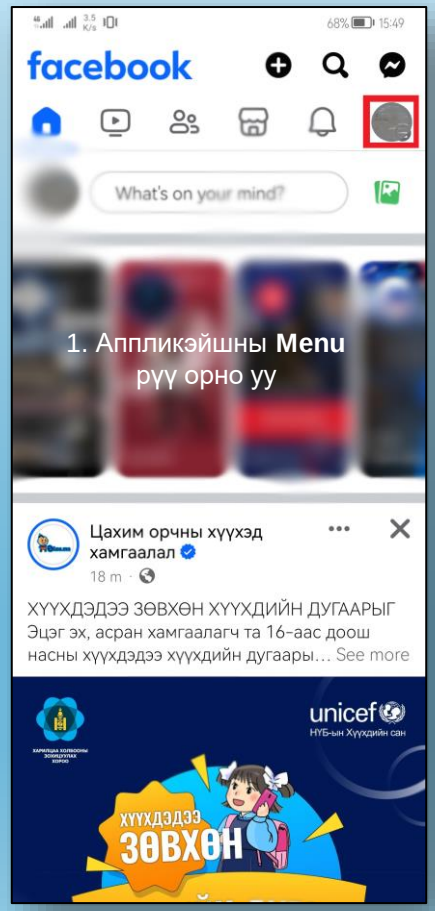
Луйварчид ихэвчлэн банк, үйлчилгээ эрхлэгч, олон нийтийн мэдээллийн хэрэгсэл гэх мэт байгууллагыг дуурайж албан ёсны мэт харагдахыг хичээдэг.

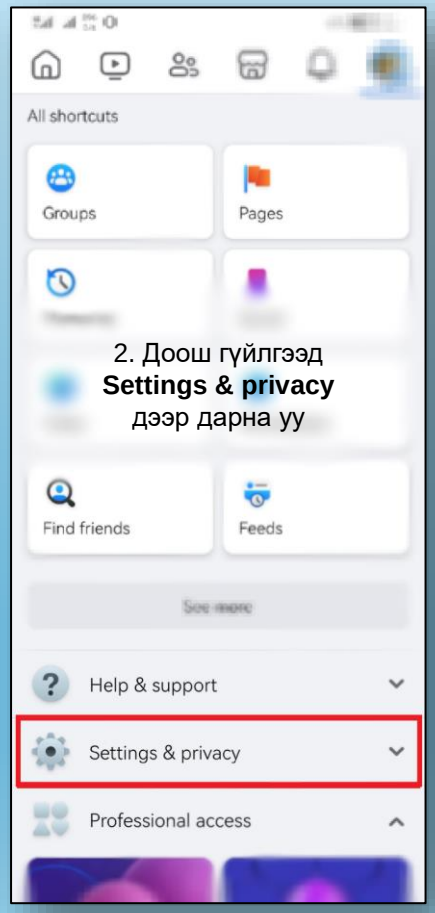
Залилан мэхлэлттэй тулгарах үед өөрийгөө хамгаалахад туслах гурван энгийн дүрэм:

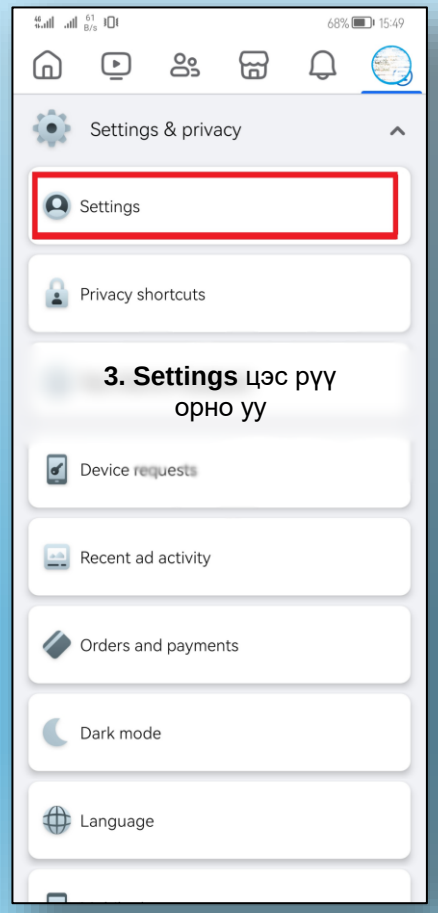
1. **Бүү яар:** Луйварчид ихэвчлэн таны бүртгэл алдагдана гэж яаралтай мэдрэмжийг бий болгодог. Асуулт асууж, өөртөө сайтар тунгаан бодох цаг гаргаарай.
2. **Шалга:** Холбоосыг дарах эсвэл файл татаж авахаасаа өмнө дэлгэрэнгүй мэдээллийг сайтар шалгаж, судалгаа хийгээрэй. Тэдний хэлж байгаа зүйлийн утга учиртай, ойлгомжтой байдлыг хянаарай.
3. **Бүү илгээ:** Луйварчид ихэвчлэн олны танил байгууллагын дүр эсгэдэг бөгөөд таныг итгүүлэхийн тулд интернэтээс хулгайлсан ажилтны зургийг ашиглаж болно. Ямар ч нэр хүндтэй байгууллага шууд төлбөр нэхэхгүй гэдгийг санаарай.

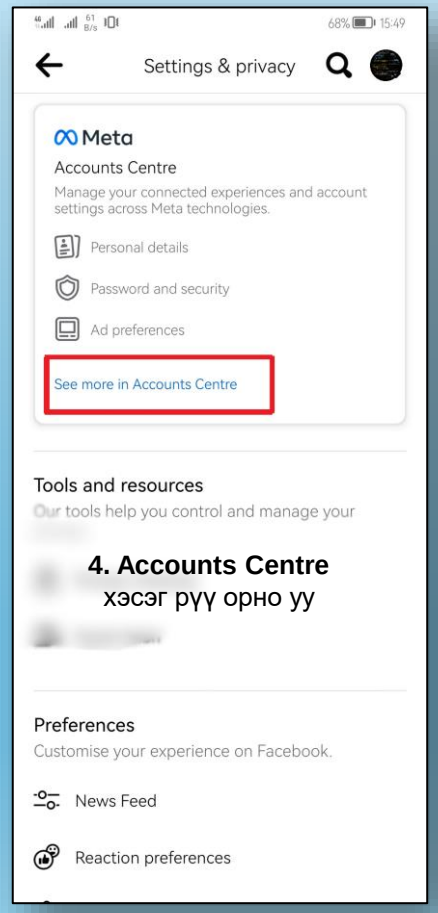
6. Сэрэмжлүүлэг болон Two-factor authentication (2FA) тохиргоог идэвхжүүлэх заавар

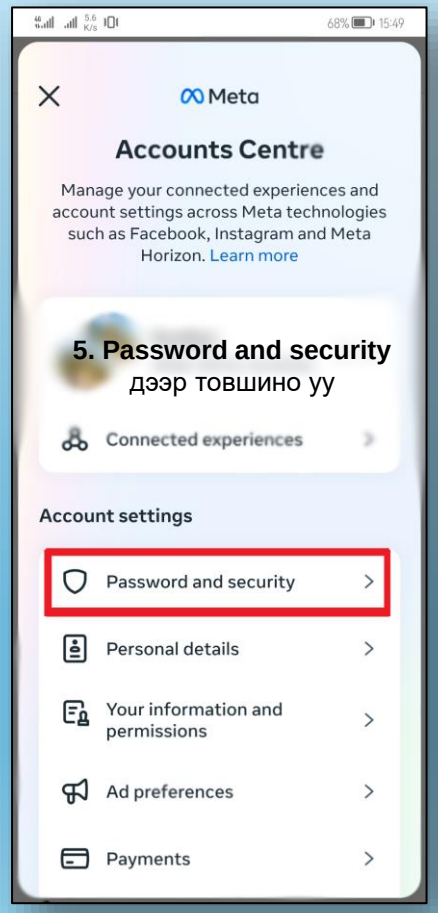
Аюулгүй байдлын тохиргооны “Password and security” цэс рүү нэвтрэх





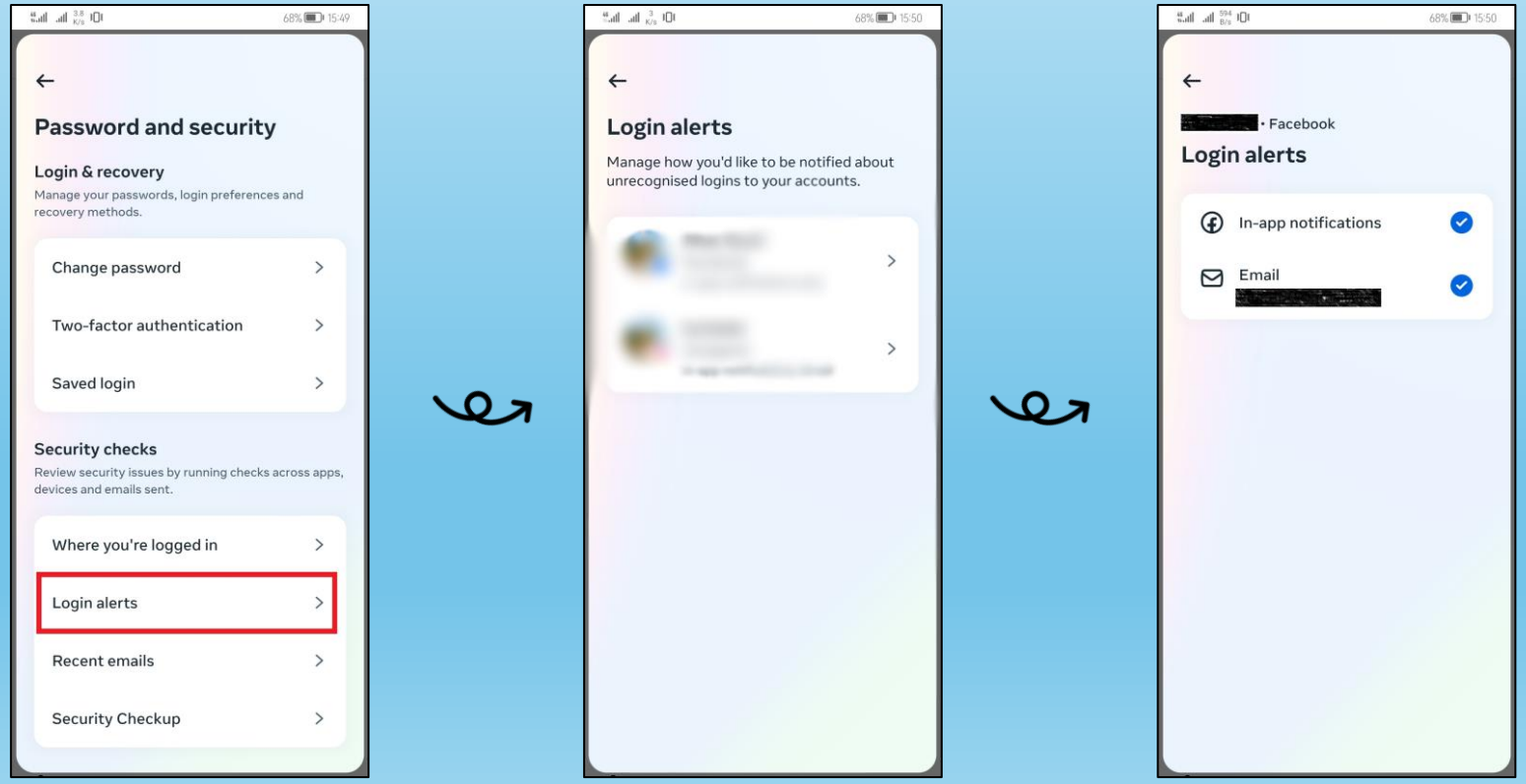






Бүртгэлгүй төхөөрөмж эсвэл вэб хөтчөөс нэвтрэхийг оролдсон тохиолдолд сэрэмжлүүлэг авах тохиргоог идэвхжүүлэх заавар

1. **Password and security** цэсний **Login alerts** сонголт дээр дарж орно уу.
2. Фэйсбүүк бүртгэлийг сонгож, өөрийн и-мэйл, аппликэйшнээр гэх мэт сэрэмжлүүлэг хүлээн авахыг хүссэн сувгийг сонгоно.

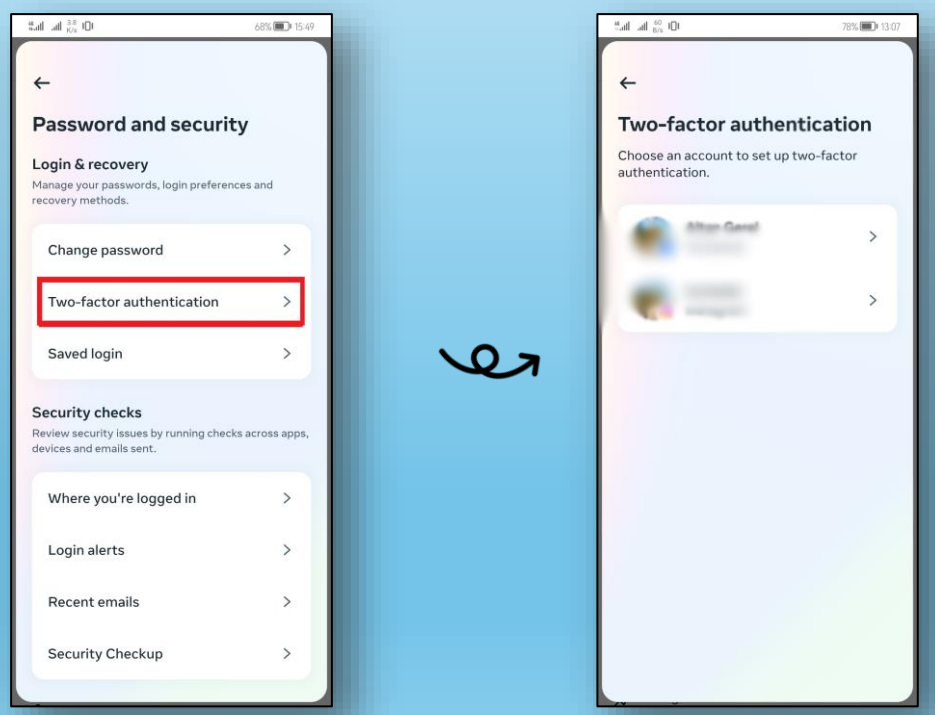


Та танигдаагүй нэвтрэлтийн талаар сэрэмжлүүлгийг идэвхжүүлснээр:

- Нэвтрэлтийн талаар мэдээлэл хүлээн аваад **This was me** дээр товшиж тухайн үйлдлийг та хийсэн гэдгийг мэдэгдэж болно.
- Хэрэв нэвтрэлтийг танихгүй бол **This wasn’t me** гэж товшсоноор танд нууц үгээ шинэчлэх, бүртгэлээ хамгаалахад тусална.
- Мөн төхөөрөмж эсвэл хөтчөө итгэмжлэгдсэн хөтөч, төхөөрөмжүүдийн жагсаалтад хадгалах боломжтой. Ингэснээр өөрийн ашигладаг компьютер эсвэл мобайл төхөөрөмжийн нэвтрэлтийн анхааруулга авахгүй. Хэрэв та номын сан, кафе гэх мэт олон нийтийн хэрэглээний компьютер ашиглаж байгаа бол дээрх жагсаалтад бүү оруулаарай.

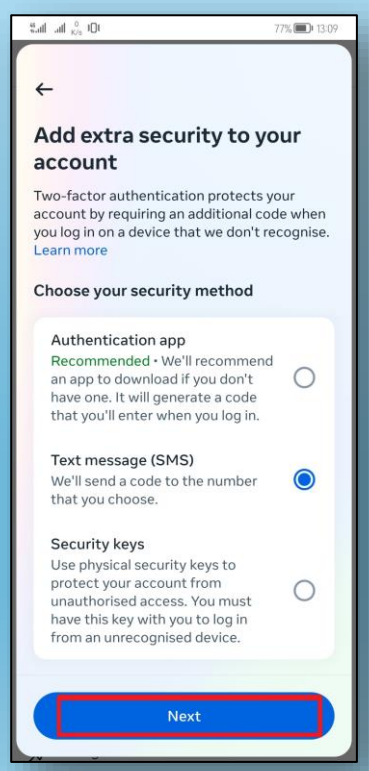
Two-factor authentication тохиргоо руу нэвтрэх

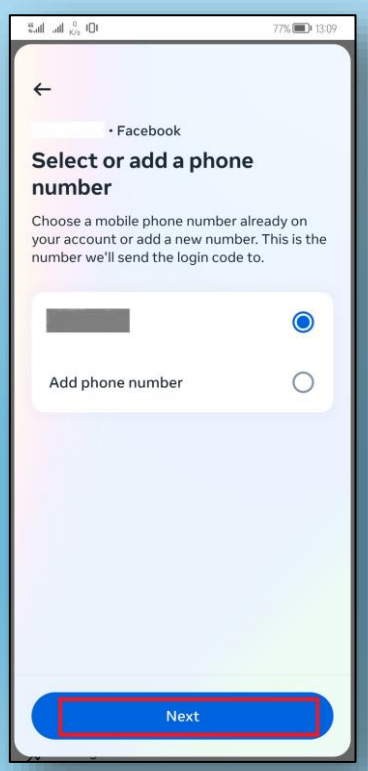
- **Two-factor authentication** цэс дээр дарж орно уу.
- Өөрийн Фэйсбүүк бүртгэлийг сонгоно уу. Энэ үед танаас нууц үгээ оруулахыг шаардана.

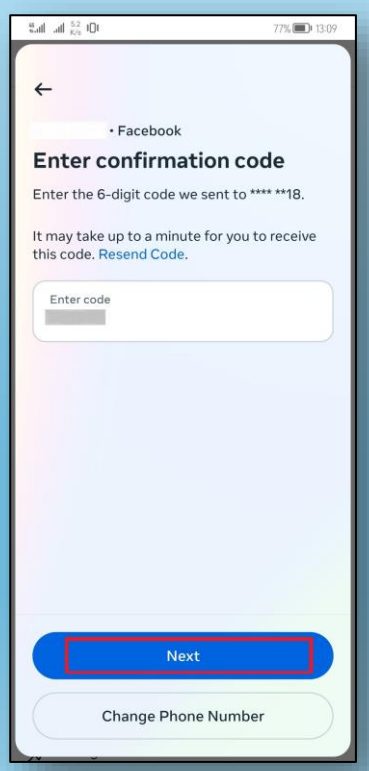


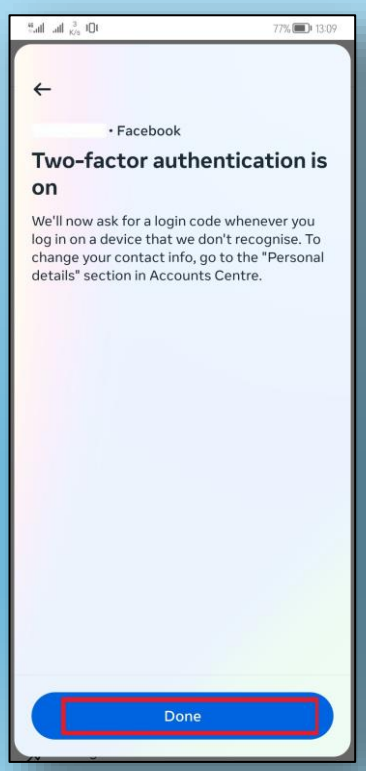
Текст мессеж (SMS) тохиргоог идэвхжүүлэх

- **Текст мессеж (SMS)** сонгож **Next** дээр дарна уу.
- Бүртгэлтэй утасны дугаар сонгох, шинэ утасны дугаар нэмээд **Next** дээр товшино уу.
- Таны утсанд баталгаажуулах код ирнэ. Тухайн кодыг аппликэйшн дээрх талбарт бөглөж **Next** дээр дарж нэвтэрнэ.
- Текст мессеж (SMS) тохиргоо идэвхжиж, **Done** товч дээр дарж дуусгана.

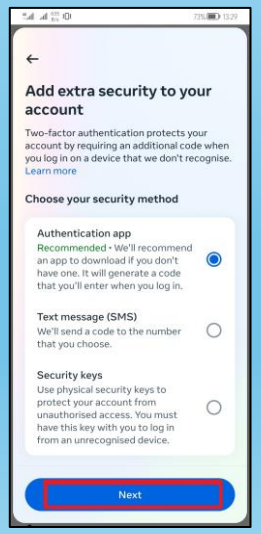


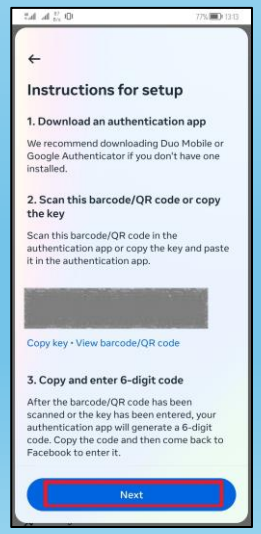


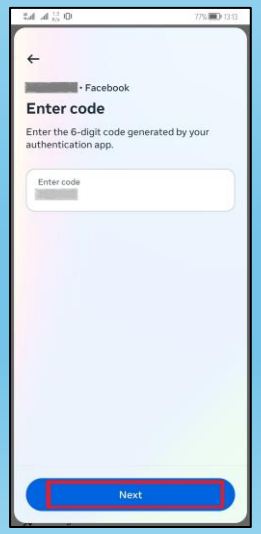


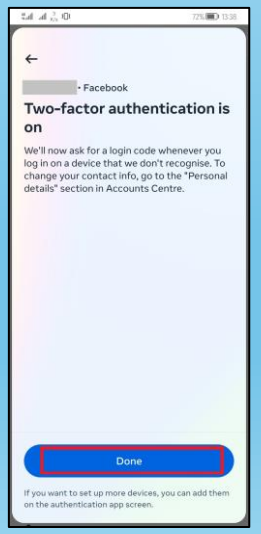


- **Баталгаажуулалтын аппликэйшнийг ашиглах**
  - **Authentication app** сонгоод **Next** дээр дарж нэвтрэх.
  - Үүний дараа баталгаажуулалтын аппликэйшнийг өөрийн ашигладаг төхөөрөмж дээрээ суулгах шаардлагатай /**Duo Mobile** эсвэл **Google Authenticator** аппликэйшнийг санал болгож байна/.
  - Фэйсбүүк аппликэйшн дээр гарч ирсэн кодыг баталгаажуулалтын аппликэйшн руу хуулах эсвэл QR кодыг баталгаажуулалтын аппликэйшн дээрээ уншуулна уу. Үүний дараа баталгаажуулалтын аппликэйшн дээр 6 оронтой код үүсэх бөгөөд та тухайн кодыг хуулж авах шаардлагатай.
  - Фэйсбүүк аппликэйшн дээрх **Next** дээр дарж нэвтэрнэ үү.
  - Баталгаажуулалтын аппликэйшнээс үүсгэсэн кодыг оруулаад **Next** дээр товшино уу.
  - Баталгаажуулалтын аппликэйшнийг ашиглах тохиргоо идэвхжих бөгөөд **Done** дээр дарж дуусгана.

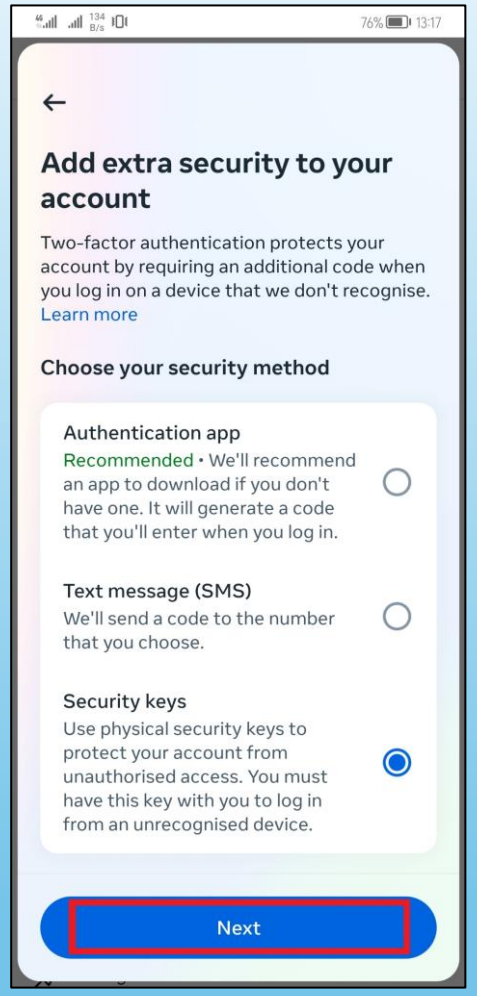


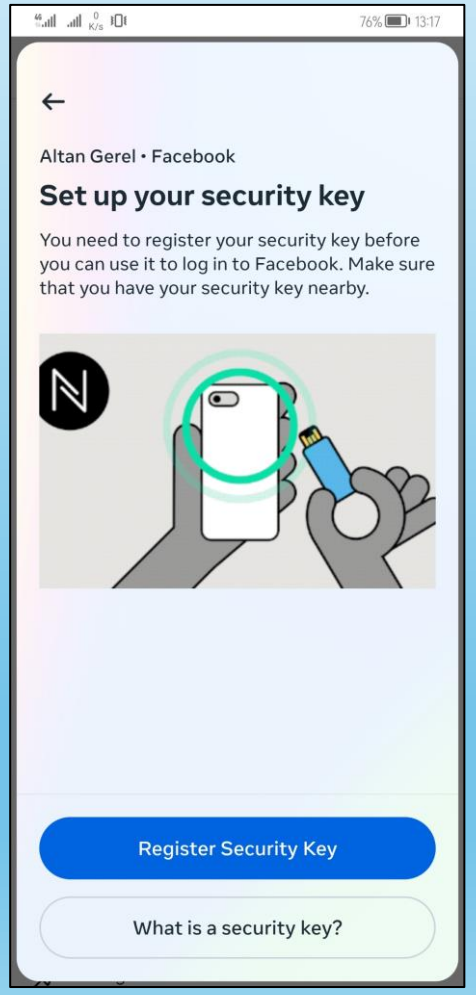






6.2. Two-factor authentication (2FA) тохиргоог удирдах





Аюулгүй байдлын түлхүүр (Security keys)-ийн тохиргоо

- Аюулгүй байдлын түлхүүр нь таны бүртгэлийг аюулгүй байлгахад туслах жижиг төхөөрөмж юм.
- Аюулгүй байдлын түлхүүрийг бүртгүүлсний дараа танигдаагүй хөтөч эсвэл төхөөрөмжөөс нэвтрэх оролдлого бүрд аюулгүй байдлын түлхүүрээр нэвтрэхийг шаардах болно.

- Та эхлээд U2F эсвэл FIDO2 аюулгүй байдлын түлхүүр худалдаж авах хэрэгтэй.
- Зарим төрлийн түлхүүрүүдийг USB эсвэл lightning портоор ашиглаж болно.
- Бусад төрлийн түлхүүрүүдийг компьютер эсвэл гар утасныхаа ойролцоо барьснаар NFC технологийг ашиглаж болно.
- Худалдан авахаасаа өмнө таны аюулгүй байдлын түлхүүр нь хөтөч болон бүртгэлдээ нэвтрэхэд ашигладаг төхөөрөмжид нийцсэн эсэхийг шалгаарай.

Аюулгүй байдлын түлхүүрээ алдсан тохиолдолд бүртгэлээ түгжихээс болгоомжлоорой

- Таны түлхүүр алдагдаж бусад хүний гарт орсон хэдий ч таны хэрэглэгчийн нэр, нууц үгийг мэдэхгүйгээр таны бүртгэл рүү нэвтрэх боломжгүй.
- Аюулгүй байдлын түлхүүрээ алдсан тохиолдолд бүртгэлээ түгжихгүй байхын тулд хоёр нөхцөлт танилт (Two-factor authentication)-ын аюулгүй байдлын нэмэлт нөөц аргыг тохируулах шаардлагатай.
- Хамгийн найдвартай арга бол өөрийн дансанд олон түлхүүр тохируулах явдал юм.

Сэргээх код тохиргоог идэвхжүүлэх

Хоёр нөхцөлт танилт (Two-factor authentication)-ын тохиргоог идэвхжүүлсэн тохиолдолд Фэйсбүүкт нэвтрэх боломжгүй болсон үед ашиглах нэг удаагийн нэвтрэх код авах боломжтой.

- **Additional methods** сонгоод **Recovery codes** дээр дарж нэвтэрнэ.
- **Turn on** дээр дарж гарч ирсэн кодуудыг хадгалж авна. Та гарч ирэх кодыг хадгалж *(screenshot)* эсвэл бичиж авч болно. Та код бүрийг зөвхөн нэг удаа ашиглах боломжтой.
- Гарах (**X**) товч дээр дарж тохиргоог дуусгана.