

ХУВИЙН ТӨХӨӨРӨМЖҮҮДЭЭ ХУЯГЛААРАЙ

УДИРТГАЛ

Бидний өдөр тутмын амьдрал технологитой салшгүй холбоотой болсон нь давуу тал төдийгүй технологийн төвөгтэй байдлуудыг ч давхар бий болгосоор байна. Технологи хурдацтай өөрчлөгдөж буй энэ цаг үед өөрийн ашиглаж байгаа цахим төхөөрөмжүүд болох компьютер, ухаалаг гар утасныхаа аюулгүй байдлыг хангах нь кибер халдлага, эрсдэлүүдээс урьдчилан сэргийлэхэд туслах чухал алхам юм. Иймд цахим төхөөрөмжүүдийнхээ аюулгүй байдлыг хангахад туслах зөвлөмжүүдийг танд хүргэе.

ҮНДСЭН АГУУЛГА

Хамрах хугацаа:	2023 оны 12-р сарын эхний хагас (#1)
Хамрах сэдэв:	Ухаалаг утас болон компьютер дээрх өгөгдлийн аюулгүй байдлыг хангахад дагаж мөрдвөл зохих тэргүүн туршлагууд
📌 Кибер аюул заналын ухаалаг утас, компьютер зэрэг хувийн төхөөрөмжид учруулж болох эрсдэлийг ойлгох нь Бид өөрсдийн хэрэглэж, эзэмшиж байгаа машин, байр байшин гэх мэт эд хөрөнгөндөө учирч болох эрсдэлүүдээс урьдчилан сэргийлэхийн тулд хэрхэх тухайгаа мэддэг буюу харуул хамгаалалттай газар машинаа орхих, түгжих, дохиолол, хяналтын камер суурилуулах зэрэг арга хэмжээг авч хэрэгжүүлдэг. Тэгвэл өнөө цагт бидний өдөр тутамдаа хэрэглэж байгаа цахим төхөөрөмжүүдийг чиглэсэн кибер аюул заналууд мөн байдаг гэдгийг ойлгох нь тэдгээр аюул заналын учруулж болох эрсдэлээс сэргийлэх эхний алхам юм. Сошиал, и-мэйл хаягаа алдсанаас үүдэж өөрт болон бусдад санхүүгийн хохирол учруулах, нууц эмзэг мэдээллээ бусдад алдах, мөн компьютер, гар утсанд янз бүрийн хортой программ, вирус сууснаас үүдэж ажлаа хэвийн гүйцэтгэх боломжгүй болох зэргээр кибер аюул заналууд нь бидэнд төрөл бүрийн асуудал учруулах эрсдэлтэй учраас өөрийн хувийн болон албан байгууллагын хэрэгцээнд ашиглаж байгаа цахим төхөөрөмжүүдийнхээ аюулгүй байдлыг хангах алхмуудыг хэрхэн авч хэрэгжүүлэх талаар дараах мэдээллүүдтэй танилцъя. 📌 Суурин болон зөөврийн компьютерынхоо аюулгүй байдлыг хангах нь 🖥 Шинэчлэлтийг тогтом хийх 🖥: Компьютерын үйлдлийн систем болон түүн дээр ажиллаж программ хангамжуудын шинэ хувилбар болон системийнхээ өмнөх	



алдааг зассан шинэчлэлт тогтмол гарч байдаг учир шинэчлэлтийг автоматаар тогтмол хийдэг болгож тохируулах

-  **Хүчтэй нууц үг ашиглах**  : Компьютер болон ухаалаг утас руугаа нэвтрэх болон тэдгээр дээрх бусад программ хангамж, веб аккаунтад хандах нууц үгийг том жижиг үсэг, тоо, тэмдэгт орсон таахад хэцүү байхаар нууц үгийг үүсгэх. Салбарын мэргэжилтнүүд болон мэргэжлийн байгууллагаас нууц үгийг хамгийн багадаа 12 тэмдэгтийн урттай байхаар сонгохыг зөвлөдөг. Нууц үгийг үүсгэхдээ өөрийн болон ойр дотын хүмүүсийн нэр, регистрийн дугаар, утасны дугаар, төрсөн он сар өдөр зэрэг хувийн мэдээллийг оролцуулахгүй байх хэрэгтэй. Нэг нууц үгийг өөр өөр программуудад олон давтаж ашиглахгүй байхыг мөн санаарай.
-  **2FA буюу давхар баталгаажуулалтыг идэвхжүүлэх**  : Давхар баталгаажуулалтыг идэвхжүүлэх боломжтой бүхий л төхөөрөмж, программ хангамж, веб аккаунтаа хэрэгжүүлэхийг зөвлөж байна. Давхар баталгаажуулалт нь та нууц үгээ амжилттай оруулсны дараа танаас өмнө нь амжилттай нэвтэрсэн төхөөрөмжөөс нэвтрэх зөвшөөрөл хүсэх, таны гар утсанд нэг удаагийн нэвтрэх код илгээх, таны өөрийн биометрик өгөгдлөөр буюу хурууны хээ, нүүр танилтаар баталгаажуулах зэрэг олон ялгаатай арга замаар хэрэгждэг. Тиймээс таны нууц үгийг олж авсан халдагч этгээд нууц үгээс гадна дараагийн алхмын баталгаажуулалтыг давах шаардлагатай болдог тул уг халдагч этгээд таны аккаунтад шууд нэвтрэх эрсдэлийг бууруулж буй юм.
-  **Биометрик баталгаажуулалт ашиглах**  : Компьютер, ухаалаг гар утас зэрэг зөөврийн төхөөрөмж рүүгээ нэвтрэхдээ хурууны хээ, нүдний нүүрний хэв зэрэг нь хүний төрөлх чанарт суурилсан дахин давтагдашгүй өгөгдлийг ашиглах нь хүчирхэг нууц үг зохиож түүнийгээ цээжлэх эсвэл нууцлалтайгаар хадгалах зэрэг төвөгтэй байдлыг хялбарчлахын зэрэгцээ аюулгүй байдлаа хангах давуу талыг бий болгоно. Тиймээс биометрик өгөгдлөөр нэвтрэх сонголтын идэвхжүүлж ашиглахыг зөвлөж байна.
-  **Шифрлэлт (encryption) ашиглах**  : Шифрлэлт гэдэг нь таны компьютер дээрх өгөгдлийг тайлж унших боломжгүй болгон нууцалдаг арга бөгөөд үүнийг ашигласнаар таны өгөгдөл алдагдсан тохиолдолд бусад таны өгөгдлийг ашиглах боломжгүй болно гэсэн үг юм. Тиймээс зөөврийн төхөөрөмжүүд дээрээ шифрлэлтийг идэвхжүүлээрэй. Ингэснээр зөөврийн төхөөрөмжөө гээсэн, алдсан үед таны төхөөрөмж дээрх өгөгдөлд бусад хандах эрхгүй байх юм.
-  **Веб хөтөч болон и-мэйлээс ирэх хортой файлаас сэргийлэх**  : Баталгаагүй эх сурвалж, веб сайтуудаас программ татаж суулгахаас зайлсхийгээрэй. Мөн и-мэйлээр ирсэн хавсралт файлд хортой код хавсаргасан байх эрсдэлтэй тул нээх болон ажиллуулахаас өмнө анти-вирусийн программаар шалгах нь зүйтэй. Ингэснээр та өөрийн төхөөрөмж элдэв бусын зорилготой хорт кодын халдвар авахаас сэргийлж чадах юм.

- **Өгөгдөл, файлаа тогтмол нөөцлөх** 🗂️: Компьютер болон ухаалаг утас дээрх файлуудаа тогтмол өөр төхөөрөмж болон үүлэн сервис дээр хуулж байх. Ингэснээр таны төхөөрөмж алдагдах эсвэл халдлагад өртөж файл руугаа хандах боломжгүй болсон үед нөөцөлсөн эх сурвалжаасаа файлаа буцааж сэргээх боломжтой юм.
- **Нийтэд нээлттэй утасгүй сүлжээнд холбогдохгүй байх** 🌐: Кофешоп, дэлгүүр гэх мэт олон нийтийн газар дахь нийтэд нээлттэй, үнэгүй утасгүй сүлжээнд өөрийн төхөөрөмжөөр холбогдохоос аль болох зайлсхийх хэрэгтэй. Учир нь халдагч этгээдүүд таны компьютерын сүлжээгээр дамжиж буй мэдээллийг цуглуулах болон хортой код агуулсан веб хуудас руу хандуулах зэрэг үйлдэл хийх эрсдэлтэй байдаг.
- **Анти-вирусийн программ ашиглах** 🛡️: Таны хийж буй аливаа үйлдлийн улмаас хортой код таны төхөөрөмж нэвтрэх эрсдэл үргэлж үүсэж байдаг. Тиймээс уг төрлийн эрсдэлээс өөрийн төхөөрөмжөө хамгаалахын тулд анти-вирусийн лицензтэй программ хангамжийг төхөөрөмждөө суулгаж, ашиглаж хэвшээрэй.
- **Төхөөрөмжийн физик аюулгүй байдлыг хангах** 🗝️: Компьютер болон зөөврийн компьютероо түгжилгүйгээр орхих нь таны компьютерт бусад этгээд зөвшөөрөлгүй хандах эрсдэлийг үүсгэдэг. Тиймээс компьютероо түр орхихдоо дэлгэцээ түгжиж хэвших нь уг эрсдэлээс сэргийлэх чухал алхам юм. Мөн зөөврийн компьютерыг хулгайд алдахаас сэргийлэхийн тулд түгжих кабель ашиглахыг зөвлөж байна.

Хамрах хугацаа:	2023 оны 12-р сарын сүүлийн хагас (#2)
Хамрах сэдэв:	Ухаалаг утасны аюулгүй байдлын зөвлөмж
🧩 Ухаалаг утас бол бидний өдөр тутамдаа хэрэглэж байгаа цахим төхөөрөмж учраас түүний аюулгүй байдлыг суурь түвшинд хэрхэн хангаж ашиглах талаар зөвлөмжүүдийг хүргэе. ■ Ухаалаг утсаа түгжих: Ухаалаг утасныхаа аюулгүй байдлыг хангах хамгийн эхний алхам бол ухаалаг утасны дэлгэцийн түгжээг идэвхжүүлж ашиглах юм. Дэлгэцийг түгжихдээ ашиглаж байгаа тухайн утасны үйлдвэрлэгч болон хувилбараас хамаараад пин код, нууц үг, паттерн түгжээ, биометрик нэвтрэлтийг ашиглах боломжтой байдаг. ■ Шинэчлэлтийг тогтмол хийх: Ухаалаг утасны үйлдвэрлэгчид болон утасны аппликейшн	



хөгжүүлэгчид тогтмол шинэ хувилбар, алдаа зассан шинэчлэлтээ гаргаж байдаг учир ухаалаг утсан дээрээ тэдгээр шинэчлэлтүүдийг автоматаар хийдэг тохиргоог нь идэвхжүүлээрэй.

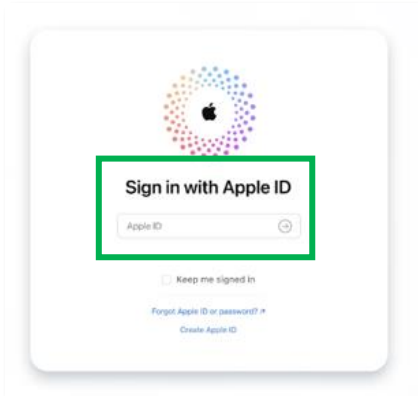
-  **Аппликейшны эрхийн тохиргоог анхаарах:** Ухаалаг утсанд шинээр аппликейшн татаж суулгах үед таны утасны тодорхой төрлийн өгөгдлүүд рүү хандаж ажиллах эрхийн хүсэлтийг асуудаг. Жишээлбэл, таны байршил, утасны контакт, мессеж, зураг гэх мэт хэсгүүд тухайн аппликэйшнаас хандах эрхийн зөвшөөрөл асуусан эсвэл хандах тухай анхааруулга мэдээллийг өгдөг. Иймд та аппликейшн суулгаж байх үедээ тэдгээр мэдээллийг анхааралтай уншиж, тухайн аппликейшны зорилгоос хамаараад зөвхөн зохих хэсэгт хандах эрхийг зөвшөөрөх байдлаар уг аппликэйшны эрхийг хязгаарлах боломжтой.
- **!? Аппликейшныг баталгаат эх сурвалжуудаас татаж суулгах:** Гар утсан дээрээ аппликейшн татаж суулгахдаа зөвхөн Google PlayStore, Apple App Store зэрэг баталгаат эх сурвалжаас татаж суулгахыг эрмэлзээрэй. Өөр баталгаагүй эх сурвалжаас аппликэйшныг татаж суулгах нь хортой кодын халдварт өртөх эрсдэлтэйг гэдгийг анхаараарай.
-  **Утасны байршил болон алсаас өгөгдөл устгах:** Ухаалаг утсаа алдсан тохиолдолд уг утас интернэтэд холболттой бол утасны байршлыг олж тогтоох эсвэл утсан дээрх мэдээллүүдээ алсаас устгах боломжтой байдаг. Хэрвээ утасныхаа байршлыг олж тогтоосон хэдий ч эргүүлэн олж авах боломжгүй бол түүн дээр хадгалсан өгөгдөл, мэдээллийг бусдын гарт орохоос сэргийлэх арга хэмжээ авах нь нэн түрүүнд хийх алхам юм. Ингэснээр хэн нэгэн таны утсан дээр байгаа өгөгдөл рүү хандах боломжгүй болно.
-  **Аюулгүй байдлын программ хангамж суулгах:** Ухаалаг утсанд зориулсан анти-вирусийн лицензтэй программ болон суулгах гэж буй аппликейшны аюулгүй байдлыг шалгах лицензтэй программ хангамж ашиглаж хэвшээрэй.
-  **Ухаалаг утсаа алдсан тохиолдолд:** Хэрэв та ухаалаг утсаа хулгайд алдсан бол цагдаад мэдэгдээрэй.
-  **Шифрлэлт (encryption) ашиглах**  : Шифрлэлт гэдэг нь таны ухаалаг утсан дээрх өгөгдлийг тайлж унших боломжгүй болгон нууцалдаг арга бөгөөд үүнийг ашигласнаар та утсаа алдсан тохиолдолд бусад этгээд таны өгөгдөлд хандах эрхгүй байх юм. Иймд ухаалаг утсан дээрээ шифрлэлтийг идэвхжүүлээрэй.

ЗААВАРЧИЛГАА

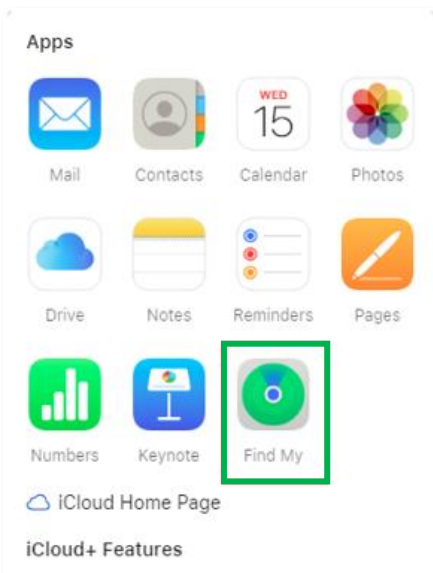
Хэрвээ ухаалаг утсаа алдсан тохиолдолд утсан дээрх нууцлалтай мэдээллээ бусдад алдахаас сэргийлж, iOS болон Android үйлдлийн системтэй утаснуудын хувьд алсаас устгах үйлдлийг хэрхэн хийх зааварчилгааг хүргье.

- ✅ **iOS үйлдлийн системтэй тохиолдолд**

1. iCloud.com сайт руу **өөрийн бүртгэлээрээ** нэвтрэнэ.



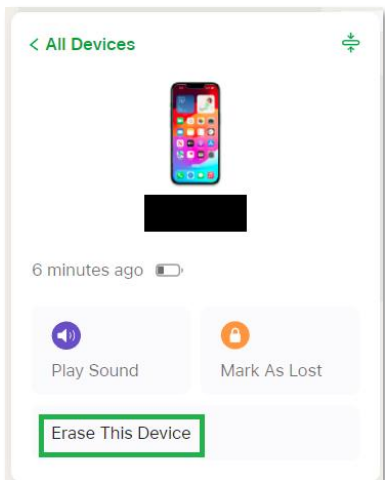
2. **Find My Devices** хэмээх аппликэшныг сонгоно.



3. Өгөгдлийг нь устгах шаардлагатай байгаа **утсаа** сонгоно

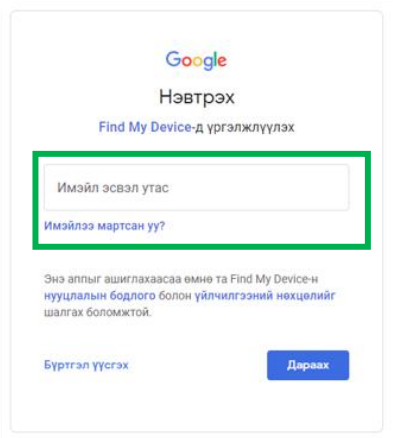


4. **Erase This Device** сонголтыг хийж, өгөгдлөө устгана.

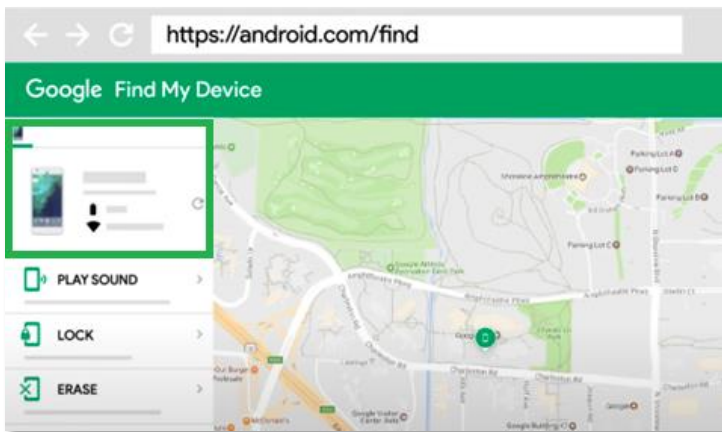


✓ **Android үйлдийн системтэй тохиолдолд**

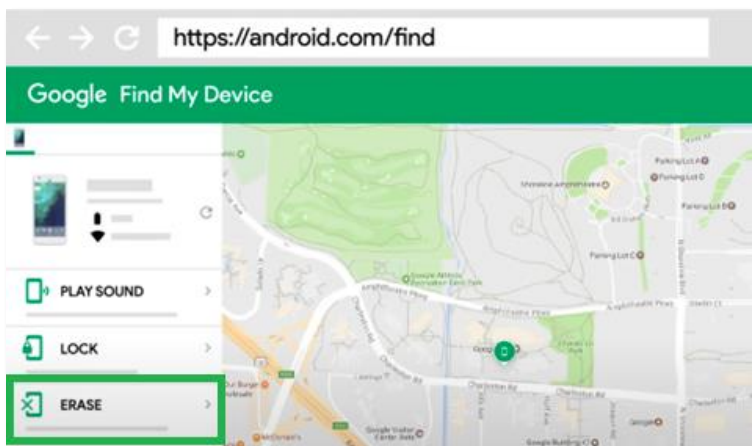
1. **Android.com/find** сайт руу **өөрийн Google бүртгэлээрээ** нэвтрэнэ.



2. Өгөгдлийг устгах шаардлагатай байгаа **утсаа** сонгоно.



3. **Erase** сонголтыг хийнэ.



ДҮГНЭЛТ

Цахим хэрэглээндээ өдөр тутамдаа ашиглаж байгаа өөрийн компьютер, ухаалаг утасныхаа аюулгүй байдлыг хангах нь нууцлалттай мэдээллээ алдах, санхүүгийн хохирол амсах, хувь хүн болон байгууллагын нэр хүндэд сөргөөр нөлөөлөх эрсдэлээс хамгаалдаг тул хувийн цахим төхөөрөмжүүддээ аюулгүй байдлыг хэрхэн хангах талаар зөвлөмжийг энэ удаагийн сэдвээр хүргэлээ.

ОЙЛГОЛТ ШАЛГАХ АСУУЛТУУД

- 1 Баталгаагүй эх сурвалжаас программ татаж суулгах нь танд ямар эрсдэлийг үүсгэж болох вэ? Хамгийн оновчтой нэг хариултыг сонгоно уу.
 - a. Компьютерын үзүүлэлт муудах.
 - b. Компьютер дээрх программууд ажиллахгүй болох.
 - c. Эрсдэл бага байдаг.
 - d. Хортой программд өртөх, санхүүгийн алдагдал хүлээх.**
- 2 Компьютер ухаалаг утасныхаа шинэчлэлтийг тогтмол хийхгүй байх нь аюулгүй байдлын хувьд ямар сул талтай вэ?
 - a. Аюулгүй байдлын алдаа нь засагдахгүй байх.**
 - b. Шинэчлэлт хийснээс болж төхөөрөмж удаашрах.
 - c. Ямар нэгэн сул тал бий болохгүй.
 - d. Шинэчлэлт хийснээс болж өгөгдөл устгах эрсдэлтэй.
- 3 Төхөөрөмждөө шифрлэлт ашиглах нь ямар давуу талтай вэ?
 - a. Цахим халдлагад өртөхгүй болгоно.
 - b. Төхөөрөмжөө алдсан тохиолдолд гаднын этгээд хандах боломжгүй.**
 - c. Файлын нэрийг өөрчилдөг.
 - d. Хортой программ суухаас хамгаална.
- 4 И-мэйлийн хавсралтаар татаж авсан файлуудын аюулгүй байдлыг хэрхэн шалгах вэ?
 - a. Файлын хэмжээгээр
 - b. Анти-вирусийн программаар шалгах**
 - c. Файлын нэрийг шалгах

d. И-мэйлээр хортой программ дамжих боломжгүй байдаг тул шаардлагагүй

5 Биометрик баталгаажуулалт гэдэг нь?

- a. Хүчирхэг нууц үг тохируулж ашиглах
- b. Пин код үүсгэж ашиглах
- c. **Хурууны хээ, нүүрний хэв танилтаар баталгаажуулах**
- d. Нэг удаагийн нууц үг ашиглах