📶 УТАСГҮЙ ЕРТӨНЦИЙН ХИЛ ХЯЗГААРАА БЭХЖҮҮЛЭХҮЙ ДОР 🔒

УДИРТГАЛ

Бидний өнөөгийн амьдралыг интернэтийн сүлжээгүйгээр төсөөлөхийн аргагүй. Учир нь гар утаснаас эхлээд ухаалаг гэрийн хэрэгслүүд гээд бидний хэрэглэдэг бүхий л үйлчилгээнүүд Wi-Fi, Bluetooth гэх мэт утасгүй сүлжээнд суурилан ажилладаг болсон байна. Бид амьдралынхаа салшгүй энэ хэрэглээний кибер аюулгүй байдлыг хангаж чадаж байгаа болов уу? Энэ асуултын хариулт болгож, Wi-Fi болон Bluetooth төрлийн утасгүй сүлжээний аюулгүй байдлыг хангахын ач холбогдлыг ойлгох, түүнийг амьдралдаа хэрэгжүүлэх практик зөвлөгөөг хүргэж байна.

ҮНДСЭН АГУУЛГА

Хамрах хугацаа:	**2024 оны 1-р сарын эхний хагас (#1)**
Хамрах сэдэв:	**Утасгүй сүлжээ (Wi-Fi, Bluetooth)-ний аюулгүй байдалд учрах эрсдэлүүд, аюулгүй байдлыг хангахын тулд авбал зохих алхмууд**

📌**Wi-Fi сүлжээний ач холбогдол, аюулгүй байдлын талаар:**

Wi-Fi бол бидний төхөөрөмжүүдийг интернэт сүлжээнд холбодог үл үзэгдэх гүүр юм. Энэ төрлийн утасгүй сүлжээ нь ашиглахад маш амар, хялбар боловч кибер аюул заналд өртөх нь их байдаг. Тиймээс Wi-Fi сүлжээний аюулгүй байдлыг чухалчилж үзэхгүй бол түгээмэл тохиолддог дараах эрсдэлүүдтэй тулгарах магадлал өндөр юм. Үүнд:

- **Мэдээлэл алдагдах:** Кибер гэмт хэрэгтнүүд хамгаалалт муутай Wi-Fi сүлжээнд халдлага хийж, хувийн болон санхүүгийн мэдээлэлд нэвтрэх боломжтой болдог. Энэ нь орцныхоо хаалгыг халдагчдад нээлттэй үлдээхтэй адил юм.
- **Зөвшөөрөлгүй хандалт хийх:** Wi-Fi-ийн хамгаалалт сул байгаа нь зөвшөөрөлгүй хэрэглэгчид таны сүлжээнд нэвтэрч, таны холболтыг удаашруулахаас эхлээд, хор хөнөөлтэй үйлдэл хийхэд хүргэж болзошгүй.
- **Төхөөрөмжүүд болон ухаалаг үйлчилгээнүүдэд чиглэсэн халдлага**: Ухаалаг утас, зөөврийн компьютер, бугуйн цаг зэрэгт хортой программ суулгах, ухаалаг гэрийн төрөл бүрийн төхөөрөмжүүд рүү Wi-Fi сүлжээгээр дамжин нэвтэрч орох, ухаалаг цоожноос эхлээд хамгаалалтын камерыг чиглэсэн халдлага хийн таны гэрийн аюулгүй байдал, нууцлалыг алдагдуулж болзошгүй.

📌 **Wi-Fi сүлжээний аюулгүй байдлыг хангах алхмууд:**

- 🔒 **Хүчтэй нууц үг ашиглах** 🔒**:** Төрсөн он сар, утасны дугаар, эсвэл wifipassword123 гэх мэтчилэн таамаглах боломжтой нууц үг ашиглахгүй байх. Өөрөөр хэлбэл Wi-Fi, Hotspot сүлжээ болон төхөөрөмжүүддээ аль болох нарийн төвөгтэй нууц үгээр баталгаажуулалт хийх мөн үйлдвэрээс тохируулагдаж ирдэг анхны нэвтрэх нэр, нууц үгийг өөрчлөхийг зөвлөж байна.
- 🔑 **WPA3 нууцлал ашиглах** 🔑**:** Таны ашигладаг Wi-Fi Router төхөөрөмж нь WPA3 нууцлал ашиглаж байгаа эсэхийг баталгаажуулаарай. Үүнээс өмнөх нууцлалын хувилбарууд нь олон тооны оролдлогоор нууц үгийг турших халдлага хийх боломжтой байдаг тул танай гэрийн эсвэл ажлын сүлжээнд холбогдох үйл явц цаг хугацаа болон нууц үгийн хүчтэй байдлаас хамаарах юм.
- 🔄 **Тогтмол шинэчлэл хийх** ⬆️: Төхөөрөмжүүдийн программын шинэчлэлт буюу update – ийг автомат горимд оруулах. Ингэснээр таныг сүүлийн үед гарах халдлагуудаас хамгаалах нэмэлт өөрчлөлтүүдийг суулгадаг.
- 👥 **Нийтийн Wi-Fi ашиглахаас татгалзах** 📶: Кофе шоп, нисэх онгоцны буудал, номын сан зэрэгт байдаг нийтийн Wi-Fi сүлжээ нь таны веб хуудас, сошиал сүлжээ, банкны мэдээлэл зэргийг хадгалж авах эрсдэлтэй байдаг тул олон нийтийн Wi-Fi эсвэл хэн нэгний ажиллуулж байгаа Wi-Fi сүлжээнд нэвтрэхгүй байх хэрэгтэй юм. Ийм сүлжээнүүд нь ихэвчлэн нууц үг ашиглахгүй нэвтрэх боломжтой байдаг. Зайлшгүй шаардлагаар ашиглах тохиолдолд, сүлжээнд холбогдоод хувийн бүртгэлүүд рүү нэвтэрч орохгүй байх эсвэл найдвартай VPN сүлжээ ашиглахыг зөвлөж байна.

📌 **Bluetooth сүлжээний аюулгүй байдлын асуудлууд:**

Bluetooth нь чихэвч, чанга яригч болон бусад дагалдах хэрэгслүүдийг хооронд нь холбох, төхөөрөмж хооронд мэдээлэл дамжуулах зорилгоор ашиглагддаг. Бид хэдийгээр сайн мэддэггүй ч Bluetooth нь дараах халдлагууд өртөмтгий байдаг. Үүнд:

- **Bluejacking:** Энэ халдлага нь халдагч этгээд таны төхөөрөмжийн Bluetooth асаалттай үед таны төхөөрөмж рүү зөвшөөрөлгүй холболт үүсгэж, файл илгээх гэх мэт үйлдлийг хийдэг ба энэ нь таны төхөөрөмж хортой программаар халдварлахаас эхлээд сэтгэл санаанд сөргөөр нөлөөлөх хүртэлх хор уршгийг учруулдаг.
- **Blueborne:** Энэ халдлага нь халдагч этгээдэд таны төхөөрөмжийг хянах, хувийн мэдээлэлд нэвтрэх зэрэг боломжийг олгодог. Улмаар халдагч этгээд таны төхөөрөмжүүдэд дурын үйлдэл хийх, Bluetooth ашиглан дамжуулж байгаа файлуудыг дундаас нь барих, өөрчилж дамжуулах гэх эрсдэлийг үүсгэдэг.

- **Smacking:** Bluetooth DOS гэж хэлэгддэг энэ халдлага нь хохирогчийн төхөөрөмж рүү олон тооны холболт үүсгэх оролдлогууд хийж төхөөрөмжийг хэт ачаалуулж, гацааж унтраадаг.
- **Car whispering:** Энэ халдлага нь халдагч этгээдэд машины Bluetooth сүлжээнд холбогдож дуу дамжуулах, системд нэвтрэх, хортой код дамжуулах зэрэг үйлдлүүдийг хийх төдийгүй, мөн машин доторх яриаг зайнаас чагнах боломжийг олгодог.
- **Headphone attack:** Халдагч этгээд Bluetooth чихэвчний микрофоноос таны ярьсан яриаг бичиж авдаг.

📌 **Bluetooth сүлжээний аюулгүй байдлыг хангах алхмууд:**

- ❌📴 **Илрүүлэлтийн горимыг унтраах** 📴❌: Bluetooth ашиглаагүй үед илрүүлэх горимыг унтраах. Ингэснээр танд очих ёсгүй файлыг хүлээж авахгүй байхаас гадна Bluetooth-ээр холбогдох нөхцөлөөр хийгддэг халдлагуудаас сэргийлж чадна.
- 🔒 **ПИН код эсвэл батлах түлхүүр ашиглах** 🔢: Bluetooth-ээр холболт үүсгэхдээ нууц түлхүүр ашиглах нь аюулгүй байдлыг чангатгахаас гадна зөвшөөрөлгүй холболт хийхээс сэргийлнэ.

🔄 **Программ хангамжийг шинэчлэх** ⬆️: Bluetooth-ээр ажилладаг төхөөрөмжүүддээ хамгийн сүүлийн үеийн программ хангамжийн шинэчлэлтүүдийг хийж аюулгүй байдлын алдааг засах нь халдлагаас хамгаалах нэг үндсэн нөхцөл юм.

Хамрах хугацаа:	**2024 оны 1-р сарын сүүлийн хагас (#2)**
Хамрах сэдэв:	**Wi-Fi болон Bluetooth сүлжээний аюулгүй байдлыг хангаж буй амжилтын түүх болон зөвлөмж**

🏆💡 Бидний өдөр тутмын амьдралдаа хэрэглэж байгаа дийлэнх төхөөрөмжүүд Bluetooth болон Wi-Fi технологийг дэмжиж ажилладаг билээ. Тиймээс эдгээр утасгүй технологийн аюулгүй байдлыг хангасан амжилттай туршлага болон зөвлөмжүүдийг хүргэж байна.

Wi-Fi сүлжээг аюулгүй ашиглах зөвлөмж:

- 🛑 **Нэвтрэх мэдээллийг танихгүй этгээдэд дамжуулахгүй байх**🗣️**:** Гэрийнхээ Wi-Fi-ийн нэвтрэх мэдээлэл болон мобайл hotspot-ийн нэвтрэх нэр, нууц үгийг бусдад дамжуулахгүй байх хэрэгтэй. Үүнээс үүдэн сүлжээний урсгалд ачаалал үүсгэхээс эхлээд таны болон бусад хүмүүсийн төхөөрөмж болон сүлжээнд хортой программ дамжих, мэдээлэл алдагдах эрсдэл учрах боломжтой юм.
- 🔒 **Wi-Fi сүлжээнд холбогдох нууцлалыг**

сайжруулах 🔒 : Хүчтэй, таамаглах боломжгүй нууц үг ашиглах. Өөрөөр хэлбэл Wi-Fi, Мобайл hotspot сүлжээ болон төхөөрөмжүүддээ аль болох нарийн төвөгтэй нууц үгээр баталгаажуулалт хийх, мөн Wi-Fi router-д WPA3 нууцлалыг ашиглахыг зөвлөж байна. Энэ нууцлалын тохиргоог ашигласнаар нэвтрэх мэдээллийг таах оролдлого хийх боломжийг хаадаг.

- 🔄 **Шинэчлэлтийг тогтмол хийх 🔄 :** Төхөөрөмж болон программын update-үүд нь шинээр хөгжүүлж оруулсан үйлдэл, боломжуудаас гадна аюулгүй байдлын цоорхойнуудыг зассан байдаг учраас эдгээр шинэчлэлтийг автоматаар хийдэг тохиргоог нь идэвхжүүлээрэй.
- 🚫 👥 **Зочны сүлжээ үүсгэх 🌐** : Ажил эсвэл гэрт ирсэн зочдыг зориулалтын сүлжээгээр нэвтрүүлэх. Ингэснээр та өөрийнхөө үндсэн сүлжээг бусдаас тусгаарлаж бусад төхөөрөмжөөс дамжих хор хөнөөлт үйлдлүүдээс хамгаалагдана.

📌 **Bluetooth сүлжээг аюулгүй ашиглах зөвлөмж:**

- 👁️ **Хэрэглээгүй үедээ унтраах 🔴 :** Машинаа зогсоолд зогсоогоод түгждэгтэй адил Bluetooth-ийг ашиглахгүй үедээ “invisible”, “non-discoverable”, “off” гэх мэт горимд шилжүүлж унтрааж байгаарай. Ийм дадал нь таны төхөөрөмжийг бүх төрлийн Bluetooth сүлжээг ашигласан кибер халдлагаас урьдчилан сэргийлэх болно.
- 🔐 **Холболт тогтоолтыг нуцлах 🛡️ :** Bluetooth ашигладаг бүх төхөөрөмжүүдийнхээ үйлдвэрээс тохируулагдсан байдаг анхны холбогдох нууц үгийг сольж улмаар цаашид ашиглах пин код эсвэл, нуцлал бүхий кодыг ашиглаж хэвшээрэй. Энэ нууц үг нь хялбар таамаглагдахгүй байх ёстой.
- 🔄 **Шинэчлэлтийг тогтмол хийх 🔄 :** Төхөөрөмж болон программын update-үүд нь шинээр хөгжүүлж оруулсан үйлдэл, боломжуудаас гадна аюулгүй байдлын цоорхойнуудыг зассан байдаг учраас эдгээр шинэчлэлтийг автоматаар хийдэг тохиргоог нь идэвхжүүлээрэй.
- 💬 **Зөвлөмжүүдийг бусдад хуваалцах 🗣️** : Та өөрийн болон, бусдад учирч болох аюулгүй байдлын асуудлуудыг ухамсарлаж дээр дурдсан зөвлөмжүүдийг гэр бүлийнхэн найз нөхдөдөө хуваалцаарай.

НИЙТИЙН WI-FI СҮЛЖЭЭНД АЮУЛГҮЙ БАЙДЛАА ХАНГАХ ЗААВАРЧИЛГАА

Болно	Болохгүй

Wi-Fi сүлжээг нууц үгээр хамгаалагдсан эсэхийг шалгах	Онлайн банкны үйлчилгээнд нэвтрэх
Өөрийн төхөөрөмжөөс Wi-Fi сүлжээнүүд рүү автоматаар холбогдох горимыг идэвхгүй болгох	Төхөөрөмжөө түгжилгүй орхих
Bluetooth-ийг хэрэглэхгүй үедээ унтраах, ялангуяа олон нийтийн газраар үйлчлүүлэх үед	Онлайн дэлгүүрээс худалдан авалт хийх, картын мэдээлэл оруулах
Зайлшгүй нийтийн Wi-Fi ашиглах тохиолдолд найдвартай VPN ашиглах	Нууцлал бүхий баримт бичиг илгээх, хүлээж авах

ДҮГНЭЛТ

2023 оны статистик тоон мэдээллээр дэлхий дахинд 20 тэрбум орчим утасгүй сүлжээ ашиглаж байгаа төхөөрөмж бүртгэгдсэн байна. Үүнээс харахад харилцаа холбооны технологийн өргөн хэрэглэгдэж буй утасгүй сүлжээний аюулгүй байдлын талаар мэдлэг ойлголттой байх нь иргэн бүрийн хувьд нэн чухал юм. Иймд цар хүрээгээрээ энэ төрлийн технологиудын дийлэнх хувийг эзэлж байгаа Wi-Fi болон Bluetooth-ийн аюулгүй байдлын ач холбогдлыг ойлгох, тэдгээрийн кибер аюулгүй байдлыг хангахад чиглэсэн практик зөвлөгөөг хүргэлээ. Эдгээр практик зөвлөмжүүдийг хэрэгжүүлэх нь энгийн мэт санагдаж байгаа ч ухаалаг төхөөрөмж ашиглагчдын аюулгүй байдлыг мэдэгдэхүйц сайжруулах нөлөөтэй юм.

ОЙЛГОЛТ ШАЛГАХ АСУУЛТУУД

1. Bluetooth сүлжээний аюулгүй байдлын хувьд "Bluejacking" гэж юу вэ?
   a. Халдагчид өгөгдөлд зөвшөөрөлгүй хандсан халдлага
   b. **Bluetooth төхөөрөмж рүү зөвшөөрөлгүй холболт үүсгэж халдах**
   c. Bluetooth холболтын хурдыг сайжруулах арга
   d. Bluetooth холболтыг нууцлах техник

2. WPA3 нь WiFi аюулгүй байдлын өмнөх технологиудтай харьцуулахад юуг сайжруулсан бэ?
   a. Илүү хурдтай байхын тулд нууц үгийн хүчирхэг байдлыг бууруулсан
   b. **Олон тооны үйлдлээр нууц үгийг таах халдлагаас хамгаалалдаг**
   c. Хязгааргүй тооны төхөөрөмжүүдийг холбох боломжтой
   d. Зөвхөн сүүлийн үеийн төхөөрөмжүүдийг дэмжиж ажилладаг

3. Нийтийн WiFi сүлжээг ашиглахын гол эрсдэл нь юу вэ?

a. Хэрэглэгч ихтэй тул интернэтийн хурд буурна.
b. Зарим вэбсайт, үйлчилгээнд нэвтрэх боломжгүй.
c. **Халдлагад өртөх, мэдээлэл алдах зэргээр кибер гэмт хэргийн хохирогч болох.**
d. Хэдхэн минут тутамд сүлжээг автоматаар тасалдаг.

4. Ашиглаагүй үед яагаад Bluetooth-г унтраах хэрэгтэй вэ?
   a. Төхөөрөмжийн батарейны ашиглалтын хугацааг хэмнэх.
   b. Бусад утасгүй төхөөрөмжүүдэд саад учруулахаас сэргийлэх.
   c. **Зөвшөөрөлгүй хандалтаас сэргийлэх болон халдлагад өртөх эрсдэлийг бууруулах.**
   d. Бусдын төхөөрөмжид автоматаар холбогдохгүй байх.

5. Ухаалаг төхөөрөмжийнхөө программын шинэчлэлтийг тогтмол хийх нь аюулгүй байдлыг сайжруулах**ад** ямар нөлөө үзүүлдэг вэ?
   a. Ажиллагааны хурдыг нэмнэ.
   b. **Аюулгүй байдлын цоорхой засагдаж халдлагад өртөх эрсдэлийг бууруулдаг.**
   c. Зөвхөн дизайн болон хэрэглэгчийн удирдлагыг сайжруулдаг тул аюулгүй байдалд ямар ч нөлөө үзүүлэхгүй.
   d. Сүлжээний хурдыг удаашруулдаг.