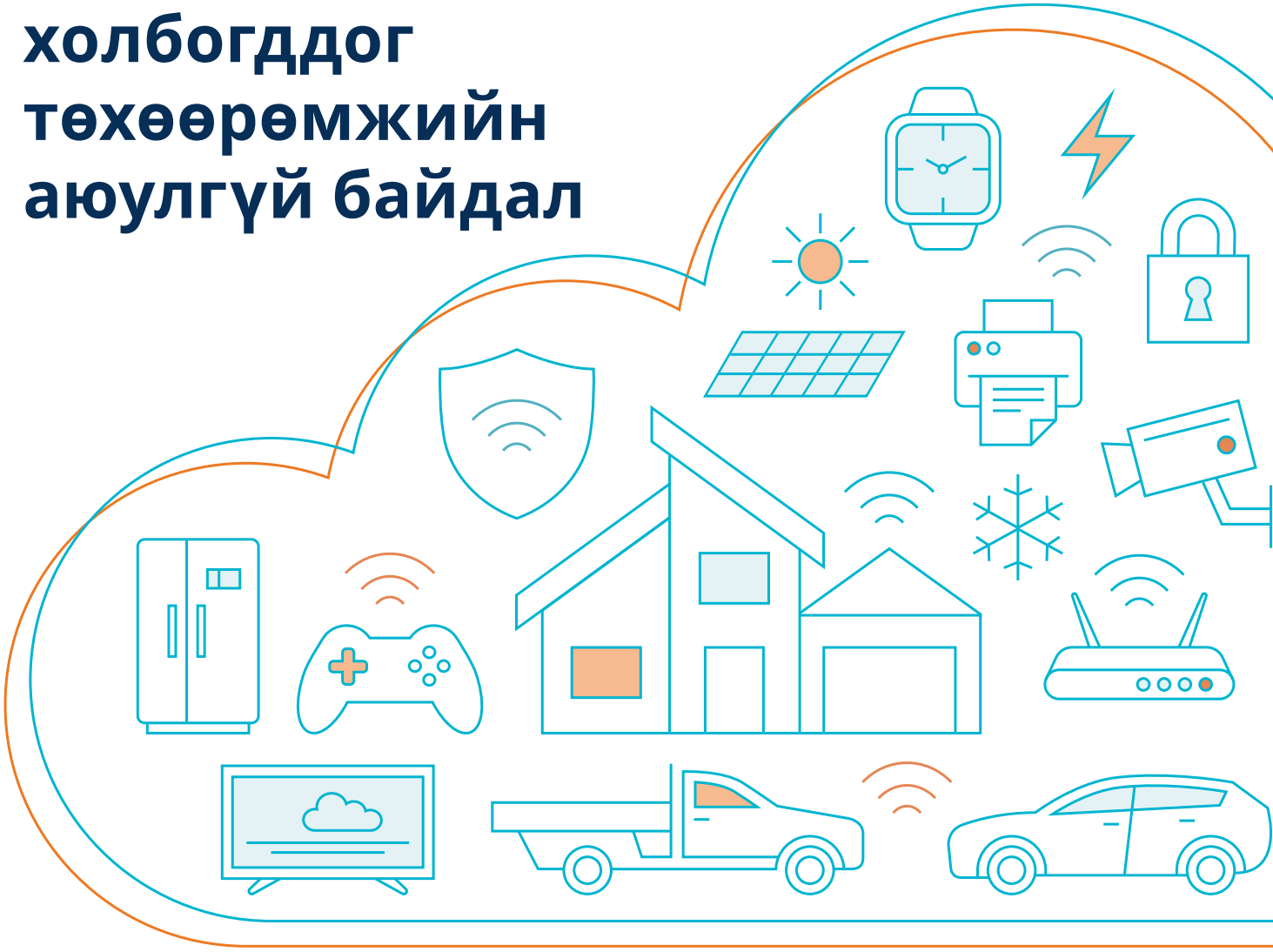
Зөвлөмж: Интернетэд холбогддог төхөөрөмжийн аюулгүй байдал



Австралийн Цахим Аюулгүй байдлын Төв нь олон нийтэд Интернетэд холбогддог төхөөрөмж (IoT)-ийг худалдан авах, аюулгүйгээр ашиглахад нь туслах зорилгоор энэхүү зөвлөмжийг боловсруулсан болно. IoT төхөөрөмж гэдэг нь интернэттэй холбогдох боломжтой өдөр тутмын хэрэглээний төхөөрөмж юм. IoT төхөөрөмжийн жишээнд нярайн хяналтын камер, дрон, аюулгүй байдлын камер, ухаалаг зурагт болон нарны эрчим хүчний хувиргагч багтана. Гэр ахуй болон бизнесийн хүрээнд ашиглагддаг IoT төхөөрөмжүүд ихэвчлэн Wi-Fi эсвэл 4G, 5G зэрэг үүрэн холбооны сүлжээг ашиглан интернэтэд холбогддог.

Австралийн айл өрхүүд болон бизнесийн байгууллагуудад түгээмэл хэрэглэгддэг олон IoT төхөөрөмжүүдийг бүтээхдээ аюулгүй байдалд төдийлөн анхаарал хандуулаагүй байдаг. Үүнээс болж эдгээр төхөөрөмжүүд интернэтээр дамжин халдлагад өртөх эрсдэлтэй байдаг. Энэ нь цахим гэмт хэрэгтнүүдэд таны төхөөрөмж болон хувийн мэдээлэлд зөвшөөрөлгүйгээр нэвтэрч, буруу зорилгоор ашиглах боломж олгодог.

IoT төхөөрөмжийг худалдан авахаасаа өмнө анхаарах зүйлс

Компаниудын үйлдвэрлэсэн бүтээгдэхүүнүүдийн аюулгүй байдлын түвшин харилцан адилгүй байдаг. Иймээс төхөөрөмж худалдан авахаасаа өмнө сайтар судлах нь чухал. Төхөөрөмж худалдан авахаасаа өмнө өөр өөр үйлдвэрлэгчдийн ижил төрлийн төхөөрөмжүүдийг харьцуулан үзээрэй. Дараах зүйлсийг анхаарвал зохино:

1. **Төхөөрөмж нь сайтар танигдсан нэр хүндтэй компанийн бүтээгдэхүүн бөгөөд албан ёсны дэлгүүрээр зарагдаж байна уу?** Сайтар танигдсан нэр хүндтэй компаниуд бүтээгдэхүүн үйлдвэрлэхдээ ихэвчлэн аюулгүй байдалд сайтар анхаардаг. Мөн нэр хүндтэй, албан ёсны дэлгүүрүүд ихэвчлэн нэр хүндтэй, алдартай компаниудын төхөөрөмжүүдийг л зөвхөн борлуулдаг бөгөөд тэдгээрийн найдвартай хангамжийн сүлжээ нь үйлдвэрлэгчийн жинхэнэ төхөөрөмжийг танд хүргэдэг.

2. **Нууц үгийг өөрчлөх боломжтой юу?** Нууц үгээ солих нь үргэлж зөв алхам байна. Хэрвээ төхөөрөмжид суулгасан анхдагч нууц үг нь сул бол үүнийг өөрчлөх нь чухал. Аюулгүй байдлыг өндөр түвшинд хангахын тулд уг төхөөрөмж нь өвөрмөц, таамаглахад бэрх, төвөгтэй, таах боломжгүй нууц үгтэй байх ёстой. Анхдагч нууц үг нь сул байвал энэ нь уг төхөөрөмж рүү халдах хамгийн хялбар арга зам болдог.

3. **Үйлдвэрлэгчийн зүгээс төхөөрөмжийнхөө програм хангамжийг шинэчилдэг эсэх?** Төхөөрөмжийн сул тал илэрсэн үед компаниуд шинэчлэлт хийж байх нь чухал юм. Жишээлбэл, хэрэв төхөөрөмжийн програм хангамжид сул тал байгаа нь илэрсэн, эсвэл халдагчид төхөөрөмжид нэвтэрч орох шинэ аргыг нээсэн бол, уг асуудлыг шийдэхийн тулд шинэчлэлт хийх шаардлагатай байдаг.

4. **Төхөөрөмж ямар мэдээлэл цуглуулах вэ, мөн цуглуулсан мэдээллийг хэнтэй хуваалцах вэ?** Төхөөрөмжийн цуглуулах өгөгдөл болон түүнийг хэрхэн ашиглах талаарх мэдээлэл нь үйлдвэрлэгчийн цахим хуудас эсвэл нууцлалын бодлогод тодорхой дурдсан байх ёстой. Онлайн эсвэл гар утасны аппликейшний цуглуулж буй мэдээлэлтэй танилцах нь үргэлж бодолцох ёстой чухал асуудал юм.

5. **Төхөөрөмж нь зөвхөн таны хүссэн үйлдлийг хийдэг үү?** Танд шаардлагатайгаас илүү функц бүхий интернэтэд холбогддог төхөөрөмжийг худалдан авах нь таны аюулгүй байдалд сөргөөр нөлөөлж болно. Төхөөрөмжийн ашиглах шаардлагагүй функцүүд нь танд ямар ч ашиггүйгээс гадна халдлагад өртөх эрсдлийг нэмэгдүүлж болзошгүй байдаг.

Интернэтэд холбогддог төхөөрөмж

Төхөөрөмжөө тохируулж байх үедээ өөрийн сүлжээ болон өгөгдлөө илүү аюулгүй байлгахад тань туслах хэдэн энгийн асуултыг санаарай.

1. **Энэ төхөөрөмж интернэтэд холбогдсон байх шаардлагатай юу?** Интэрнэтэд холбогдох боломжтой гэдэг нь заавал холбох ёстой гэсэн үг биш. Интернэтэд холбогдоогүй төхөөрөмжүүд халдлагад өртөх магадлал бага байдаг. Хэрэв та интернэт шаардах функцийг нь ашиглахгүй гэж байгаа бол тухайн төхөөрөмжийг заавал интернэтэд холбох хэрэгтэй эсэхийг эргэцүүлээрэй.

2. **Төхөөрөмж аюулгүй газар байрлаж байна уу?** Хэрвээ төхөөрөмжийг аюулгүй бус газар суурилуулах шаардлага танд байхгүй бол аюулгүй газар суурилуулах нь уг төхөөрөмжийн эвдрэл гэмтэл хулгайд өртөх эрсдэлийг бууруулна.

3. **Төхөөрөмжийн анхдагч хэрэглэгчийн нэр, нууц үгийг солих уу?** Хүчтэй нууц үг эсвэл нууц өгүүлбэр ашиглах нь чухал юм. Хэрэв таны төхөөрөмж өвөрмөц, таамаглахад хэцүү, нарийн төвөгтэй, таах боломжгүй анхдагч нууц үгтэй ирээгүй бол нууц үгийг заавал солих хэрэгтэй. Анхдагч хэрэглэгчийн нэр, нууц үгсийг цуглуулж, онлайнд нийтэлдэг тул таны төхөөрөмжийн сул тал болох эрсдэлтэй.

4. **Миний Wi-Fi сүлжээ аюулгүйгээр тохируулагдсан уу, аюулгүй нууц үгтэй юу?** Та өөрийн төхөөрөмж болон сүлжээнд гадны этгээдийг нэвтрүүлэхгүйн тулд Wi-Fi сүлжээ болон чиглүүлэгчийн аюулгүй байдлыг хангаарай.

Нэмэлт арга хэмжээ авах нь

Зөвхөн IoT төхөөрөмжүүдэд зориулсан нэмэлт Wi-Fi сүлжээг бий болгож чиглүүлэгч дээрээ тохируулна уу. Улмаар үүнийгээ Wi-Fi чиглүүлэгч дээр “зочны” сүлжээ гэж нэрлэж болно. Хэрвээ таны IoT төхөөрөмжүүд хоорондоо мэдээлэл солилцох шаардлагагүй бол “харилцагч тусгаарлалт” гэдэг функцийг идэвхжүүлээрэй. Таны IoT төхөөрөмжүүдийг нууцлал бүхий өгөгдлөөс тусгаарласнаар уг IoT төхөөрөмж халдлагад өртсөн ч таны бусад төхөөрөмж эсвэл өгөгдөлд нэвтрэх боломжийг хязгаарлах болно.

5. **Төхөөрөмжийнхөө ашиглахгүй функцүүдийг унтраасан уу?** Хэрэв таны төхөөрөмжид хэрэгцээгүй эсвэл шаардлагагүй функцүүд (жишээ нь камер, микрофон) байвал эдгээрийг аль болох унтрааж байх хэрэгтэй.

Нэмэлт арга хэмжээ авах нь

Төхөөрөмжийн веб удирдлагын интерфейсийг тухайн сүлжээний LAN эсвэл WAN/интернэтээс алсаас хандах боломжийг идэвхжүүлэх тохиргоотой эсэхийг олж мэдээрэй. Улмаар хэрвээ та уг төхөөрөмждөө алсаас хандах шаардлагагүй бол төхөөрөмжөө зөвхөн тухайн сүлжээний LAN-гаар дамжуулан ашиглаж байхаар тохируулаарай.

IoT төхөөрөмжийг зохистой хэрэглэх

Та IoT төхөөрөмжөө тохируулж, ашиглаж эхэлсний дараа дараах зүйлсийг санаарай. Үүнд:

1. **Төхөөрөмжүүдээ тогтмол унтрааж асааж байх.** IoT төхөөрөмжийн ажиллагаа удааширч эсвэл ажиллахгүй байгаа бол халдлагад өртсөн байх магадлалтай. Ихэнх хортой програм нь төхөөрөмжийн санах ойд хадгалагддаг бөгөөд төхөөрөмжийг дахин ачаалах, өөрөөр хэлбэл унтрааж асаах замаар хялбархан устгаж болно. Хэрвээ төхөөрөмжийг дахин ачаалсны дараа ч удаан эсвэл ажиллахгүй хэвээр байвал үйлдвэрийн анхдагч тохиргоог сэргээж үзээрэй, гэхдээ ингэснээр уг төхөөрөмж дэх таны бүх өгөгдөл, хувийн тохиргоо устана гэдгийг анхааараарай.

2. **Төхөөрөмждөө тогтмол шинэчлэл хийж байх.** Зарим төхөөрөмжүүдийн шинэчлэлт автоматаар хийгддэг. Автоматаар шинэчлэл хийдэггүй төхөөрөмжүүдийн хувьд үйлдвэрлэгчтэйгээ тогтмол харилцаж, шинэчлэл гарсан үед шинэчлэл хийж байна уу. Төхөөрөмжөө дахин шинэчлэх боломжгүй болсон тохиолдолд шинэчлэлтүүдийг хүлээн авах боломжтой шинэ төхөөрөмж худалдан авах талаар бодож үзээрэй. Аюулгүй байдлын шинэчлэлт хийж болохгүй төхөөрөмжүүдийн хувьд шинэ сул талууд илэрсэн үед халдлагын эрэг хамгаалалт байхгүйгээс ийм төхөөрөмжүүд таны сүлжээ, хувийн нууцлал болон өгөгдөлд эрсдэл учруулах магадлалтай.

3. **Төхөөрөмжөө ашиглахгүй үед унтраагаарай.** Ашигладаггүй, эсвэл хяналтгүй төхөөрөмжүүдийг урт хугацаагаар асаалттай байлгаж, Wi-Fi сүлжээнд холбосон байвал энэ нь таны төхөөрөмжүүдийн халдлагад өртөх магадлалыг нэмэгдүүлдэг. Төхөөрөмжийг автоматаар унтраах нэг арга нь цахилгааны залгуурын цаг тохируулагч ашиглан зөвхөн тодорхой цагуудад уг төхөөрөмжийг асаалттай байхаар тохируулах юм.

4. **Таны интернэтийн сарын хэрэглээ эсвэл төлбөр ихэссэн эсэхийг анхааралтай ажиглаарай.** Интернэтийн хэрэглээ эсвэл төлбөрийн хэмжээ огцом ихсэх нь таны төхөөрөмж халдлагад өртсөн байж болзошгүйг илтгэдэг. Хэрэв энэ асуудлыг танай байгууллагын IT хэлтэс шалгах боломж байхгүй бол төхөөрөмжийнхөө үйлдвэрийн тохиргоог сэргээж (гэхдээ энэ нь таны бүх өгөгдөл болон хувийн тохиргоог устгахыг анхааараарай), дараа нь нууц үгээ солих хэрэгтэй.

IoT төхөөрөмжийг хаях

Төхөөрөмжийг хаях эсвэл зарж борлуулах нь бусдад таны хувийн мэдээлэл болон өгөгдөлд хялбархан нэвтрэх эсвэл гартаа оруулах боломж олгож болзошгүй.

Үүнээс урьдчилан сэргийлэх арга замууд нь:

1. **Бүх өгөгдөл болон хувийн мэдээллийг устгах.** Үйлдвэрлэгч нь төхөөрөмж болон түүнд холбогдсон аппликейшнүүдээс өөрийн өгөгдөл, хувийн мэдээллийг хэрхэн устгах зааварчилгааг өгөх ёстой. Хувийн мэдээллээ устгаснаар уг төхөөрөмжийг хаясны дараа хэн ч мэдээллийг гартаа оруулах боломжгүй болно. IoT төхөөрөмжийг ашиглахгүй болсноор түүнтэй холбоотойгоор үүсгэсэн таны онлайн аккаунт хэрэгцээгүй болсон бол мөн адил устгаарай.

2. **Төхөөрөмжийн үйлдвэрийн анхдагч тохиргоог сэргээх үйлдэл хийх.** Үйлдвэрийн тохиргоог сэргээх нь төхөөрөмжийн санах ойд байгаа өгөгдлийг устгаж, нууц үг, хэрэглэгчийн нэр болон тохиргоог анхдагч байдлаар буцаах зориулалттай. Үйлдвэрийн тохиргоог хэрхэн сэргээх талаар мэдээлэл авахын тулд төхөөрөмжийн гарын авлага эсвэл үйлдвэрлэгчийн вебсайтаас шалгаарай.

3. **Төхөөрөмжийг гар утас болон бусад төхөөрөмжүүдээс салгаарай.** Өөрийн бусад төхөөрөмжүүд, сүлжээ эсвэл аккаунт руу нэвтрэх боломжтой төхөөрөмжийг хаях нь бусдад таны мэдээлэлд нэвтрэх боломж олгож болзошгүй. Хаях гэж буй төхөөрөмжтэй холбогдсон бусад төхөөрөмжүүдээ шалгаж, холболтуудыг устгасан эсэхээ баталгаажуулаарай. Гар утасны аппликейшнд олгосон ч одоо хэрэггүй болсон эрхүүдийг устгаарай.

4. **Төхөөрөмжид холбогдсон салгаж болох өгөгдөл хадгалах төхөөрөмжүүдийг (жишээ нь USB флэш драйв, санах ойн карт гэх мэт) авааарай.** Салгаж болохтөхөөрөмжүүд дээрх өгөгдөл нь үйлдвэрийн тохиргоог сэргээх үед устгагдахгүй байж болох тул тэдгээрийг биечлэн салгаж устгах болон төхөөрөмжөөс тусад нь хаях ёстой.

Дэмжлэг туслалцаа авах

Австралийн Радиотехникийн Газрын харьяа Австралийн Цахим Аюулгүй Байдлын Төвтэй холбогдохыг хүсвэл asd.assist@defence.gov.au хаягаар имэйл илгээх эсвэл яаралтай тусламж авахын тулд 24/7 дуудлагын төвд **1300 CYBER1 (1300 292 371)** дугаар руу залгаарай.

Цахим гэмт хэргийг ReportCyber сайтад www.cyber.gov.au/report хаягаар мэдээлнэ үү.

Хэрэв та хувийн мэдээллээ алдсан бол www.idcare.org сайтаар дамжуулан IDCARE-тэй холбогдоорой.

Та болон танай гэр бүлийнхэнд зориулсан зөвлөгөө авахыг хүсвэл www.cyber.gov.au сайтад зочлоорой. Сүүлийн үеийн онлайн аюул эрсдлийн талаар үнэгүй ACSC сэрэмжлүүлгийн үйлчилгээнд бүртгүүлээрэй.

Австралийг цахим орчин дахь хамгийн аюулгүй газар болгоцгооё.

Цахим аюулгүй байдлын зөвлөгөө авахыг хүсвэл www.cyber.gov.au сайтад зочлоорой.

Хариуцлагаас татгалзах мэдэгдэл

Энэхүү гарын авлага нь ерөнхий мэдээллийг агуулсан бөгөөд хууль зүйн зөвлөгөө гэж үзэхгүй ба тодорхой нөхцөл байдал эсвэл яаралтай үед тусламж авахад түшиглэх ёсгүй болно. Ямар нэгэн чухал асуудал үүссэн бол өөрийн нөхцөл байдалд тохирсон, бие даасан мэргэжлийн зөвлөгөөг авахыг зөвлөж байна.

Энэхүү гарын авлагад багтсан мэдээлэлд тулгуурлан хийсэн тодорхой үйлдлээс улбаалсан аливаа хохирол, алдагдал, зардлыг Холбооны улс хариуцахгүй.

Зохиогчийн эрх

Төрийн сүлдийг ашиглах эрх

Төрийн сүлдийг ашиглах нөхцөлийн талаарх дэлгэрэнгүй мэдээлэл болон зааврыг Ерөнхий сайд ба Засгийн газрын Тамгын газрын вебсайт Commonwealth Coat of Arms Information and Guidelines | pmc.gov.au дээрээс авна уу.

Дэлгэрэнгүй мэдээлэл авах эсвэл цахим аюулгүй байдлын хэргийгтохиолдлыг мэдээлэх бол бидэнтэй холбогдоно уу:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

Энэ дугаарыг зөвхөн Австралийн дотор ашиглах боломжтой.

AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre