PUBLIC CSIRT/CC

CYBER READ

КИБЕР АЮУЛГҮЙ БАЙДЛЫН ШИНЭ ЭМЗЭГ БАЙДЛУУД

CYBERSAFE GIRLS 2025
Stay Smart, Stay Safe

“КИБЕР ДИПЛОМАТ АЖИЛЛАГАА”
СУДАЛГААНЫ ӨГҮҮЛЭЛ

lorem ipsum dolor sit

МЭНДЧИЛГЭЭ

Захирал **Э.АМАРСАНАА**

"Кибер халдлага зөрчилтэй тэмцэх нийтийн төв" УТҮГ

Кибер аюулгүй байдлыг хангах үйл ажиллагаа нь зөвхөн мэргэжлийн байгууллагын үүрэг бус, харин төр, хувийн хэвшил, иргэн бүрийн хамтын оролцоо, хариуцлагад суурилсан цогц тогтолцоо байх шаардлагатай юм.

Та бүхэнд энэ өдрийн мэндийг дэвшүүлье.

Цахим шилжилт эрчимжиж өдөр тутмын үйл ажиллагаа мэдээллийн технологид тулгуурлах болсон өнөө үед кибер аюулгүй байдал нь үндэсний аюулгүй байдал, эдийн засгийн тогтвортой хөгжилтэй шууд холбоотой стратегийн чухал асуудал болоод байна. Ялангуяа онц чухал мэдээллийн дэд бүтэцтэй байгууллагууд нь улс орны нийгэм, эдийн засгийн тасралтгүй үйл ажиллагааг хангах суурь тулгуур учраас тэдгээрт чиглэсэн кибер халдлага, зөрчлийн тоо, төрөл жилээс жилд өсөн нэмэгдэж байна. Фишинг, хортой код, DDoS халдлага, мэдээллийн бүрэн бүтэн байдал болон нууцлалд халдах оролдлого зэрэг нь зөвхөн байгууллагуудыг бус иргэн бүрийг шууд болон шууд бусаар эрсдэлд оруулж байна.

Манай байгууллагын зүгээс кибер халдлага, зөрчлийг илрүүлэх, таслан зогсоох, хариу арга хэмжээ авах, урьдчилан сэргийлэх чиглэлээр тасралтгүй ажиллаж, иргэн, хуулийн этгээдэд кибер халдлага, зөрчлийн талаар зөвлөмж, шаардлага хүргүүлэн ажиллаж байна. Үүний зэрэгцээ олон нийтэд чиглэсэн мэдлэг, ойлголтыг нэмэгдүүлэх, цахим зөв дадлыг төлөвшүүлэх нь бидний тэргүүлэх зорилтын нэг билээ.

Энэхүү сэтгүүлийн дугаараар дамжуулан та бүхэнд кибер халдлага, зөрчлийн өнөөгийн нөхцөл байдал, тулгамдаж буй сорилтууд, цаашдын чиг хандлага, мөн иргэн, байгууллага бүрийн хэрэгжүүлэх боломжтой бодит зөвлөмжүүдийг хүргэж байна. Энэ нь зөвхөн мэдээлэл өгөхөөс гадна хамтын ойлголцол, хамтын хариуцлагыг бэхжүүлэхэд хувь нэмэр оруулна гэдэгт итгэлтэй байна.

ШИНЭ ЭМЗЭГ БАЙДЛУУД ИЛРҮҮЛЛЭЭ

Кибер халдлага зөрчилтэй тэмцэх нийтийн төв УТҮГ-ын Кибер халдлагад хариу үзүүлэх газрын албан хаагчид нээлттэй эхийн программ хангамжийн орчинд хамаарах аюулгүй байдлын эмзэг байдлыг илрүүлж, **олон улсын CVE (Common Vulnerabilities and Exposires) албан ёсны бүртгэлд** бүртгүүллээ.

МАНАЙ БАГ

Б.Билгүүндалай

Халдлагад хариу үзүүлэх шинжээч

В.Батзаяа

Тоон ул мөрийн шинжээч

П.Цэрэнпунцаг

Халдлагад хариу үзүүлэх мэргэжилтэн

ОНЦЛОХ ҮЗҮҮЛЭЛТ

12 илрүүлсэн эмзэг байдал

10/10 өндөр эрсдэлтэй (critical) эмзэг байдал

Нээлттэй эхийн программ хангамжийн аюулгүй байдлыг сайжруулахад бодит хувь нэмэр оруулж байна.

ИЛРҮҮЛСЭН ЭМЗЭГ БАЙДЛУУД

CVE ID	SEVERITY	CVSS* SCORE
CVE-2026-30921	CRITICAL	CVSS 10/10
CVE-2026-33396	CRITICAL	CVSS 9.9/10
CVE-2026-32094	CRITICAL	CVSS 9.8/10
CVE-2026-31881	CRITICAL	CVSS 9.8/10
CVE-2026-29183	CRITICAL	CVSS 9.3/10
CVE-2026-30920	HIGH	CVSS 8.6/10
CVE-2026-34524	HIGH	CVSS 8.3/10
CVE-2026-34522	HIGH	CVSS 8.1/10
CVE-2026-35205	HIGH	CVSS 7.8/10
CVE-2026-29112	HIGH	CVSS 7.5/10
CVE-2026-2950	MEDIUM	CVSS 6.5/10
CVE-2026-32828	MEDIUM	CVSS 4.9/10

*CVSS (Common Vulnerabilities and Exposires) оноо нь эмзэг байдлын эрсдэлийн түвшинг илэрхийлнэ.

ҮР ДҮН

КХЗТНТ-ийн албан хаагчид нээлттэй эхийн программ хангамжийн орчинд хамаарах 13 эмзэг байдлыг илрүүлж, олон улсын CVE бүртгэлд албан ёсоор бүртгүүлэв.

Илрүүлсэн эмзэг байдлын мэдээллийг мэдээлэх (Responsible Disclosure) зарчмын хүрээнд холбогдох хөгжүүлэгчид болон байгууллагуудад мэдээлж, эрсдэлийг бууруулах арга хэмжээг хэрэгжүүлэхэд дэмжлэг үзүүллээ.

Нээлттэй эхийн программ хангамжийн аюулгүй байдлыг сайжруулахад бодит хувь нэмэр оруулж, албан хаагчдын мэргэжлийн ур чадвар олон улсын түвшинд үнэлэгдэв.

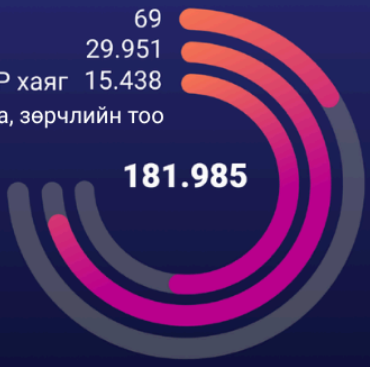
МОНГОЛ УЛСЫН КИБЕР ОРЧИН ДАХЬ 2026 АЮУЛ ЗАНАЛ

нөхцөл байдлын I улирлын тойм мэдээ

(2026.03.27-2026.04.02)

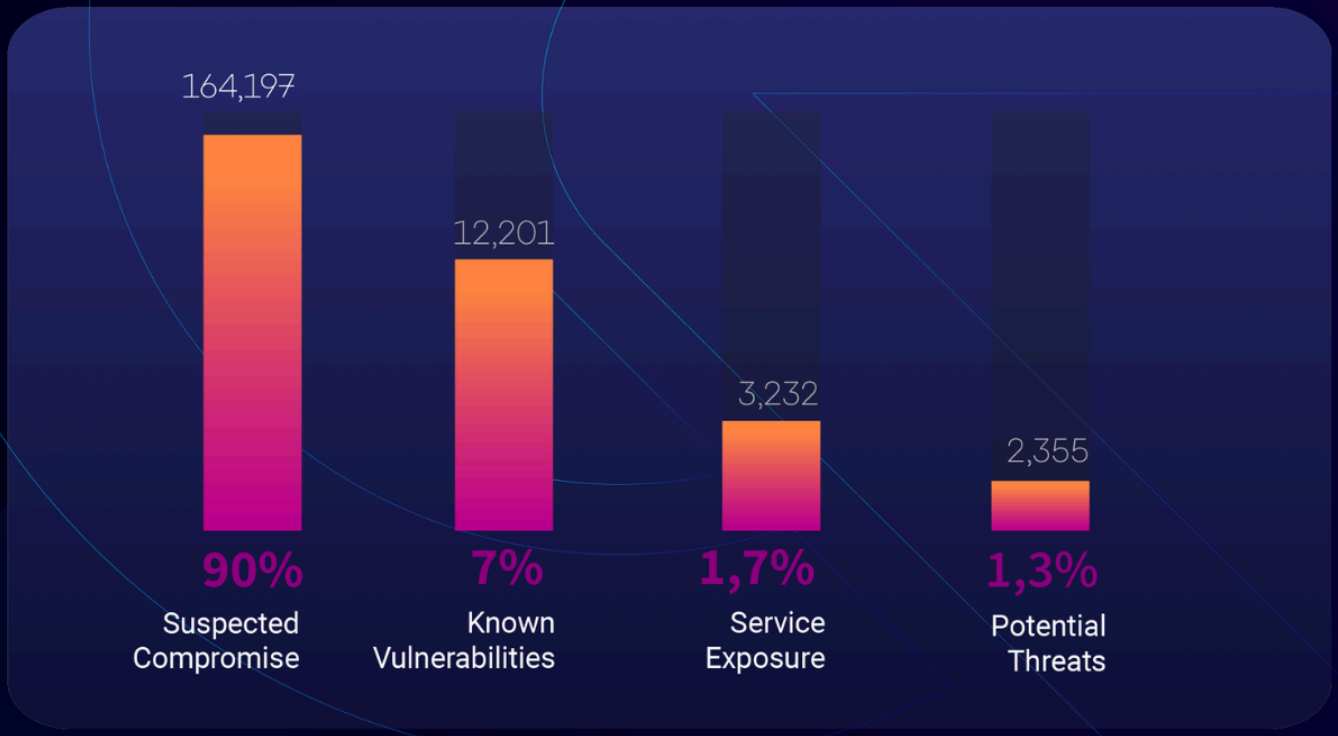
нийт халдлагын тоон үзүүлэлт

Тоологдсон ISP	69
IP хаяг (давтагдаагүй)	29.951
Гадагш репорт хийсэн IP хаяг	15.438
Нийт бүртгэгдсэн халдлага, зөрчлийн тоо	181.985



Кибер халдлага, зөрчилтэй тэмцэх нийтийн төвөөс Монгол Улсад бүртгэлтэй IP хаягуудад харгалзах сүлжээний траффикт илэрсэн сэжигтэй үйлдэл, халдлага, зөрчлийн индикаторт суурилан Монгол Улсын кибер орчин дахь аюул занал, эмзэг байдал, түүний нөхцөл байдлыг тодорхойлсон болно.

ЭМЗЭГ БАЙДЛЫГ ТӨРЛӨӨР НЬ ХАРУУЛАВ

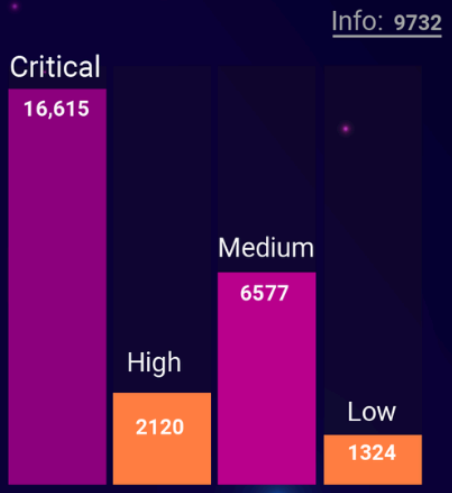


Кибер халдлага, зөрчилтэй тэмцэх нийтийн төв

ЭМЗЭГ БАЙДЛЫН ТҮВШИН

Тус хугацаанд бүртгэгдсэн кибер халдлага, зөрчлүүдийг ноцтой байдлын түвшнээр ангилан харуулав.

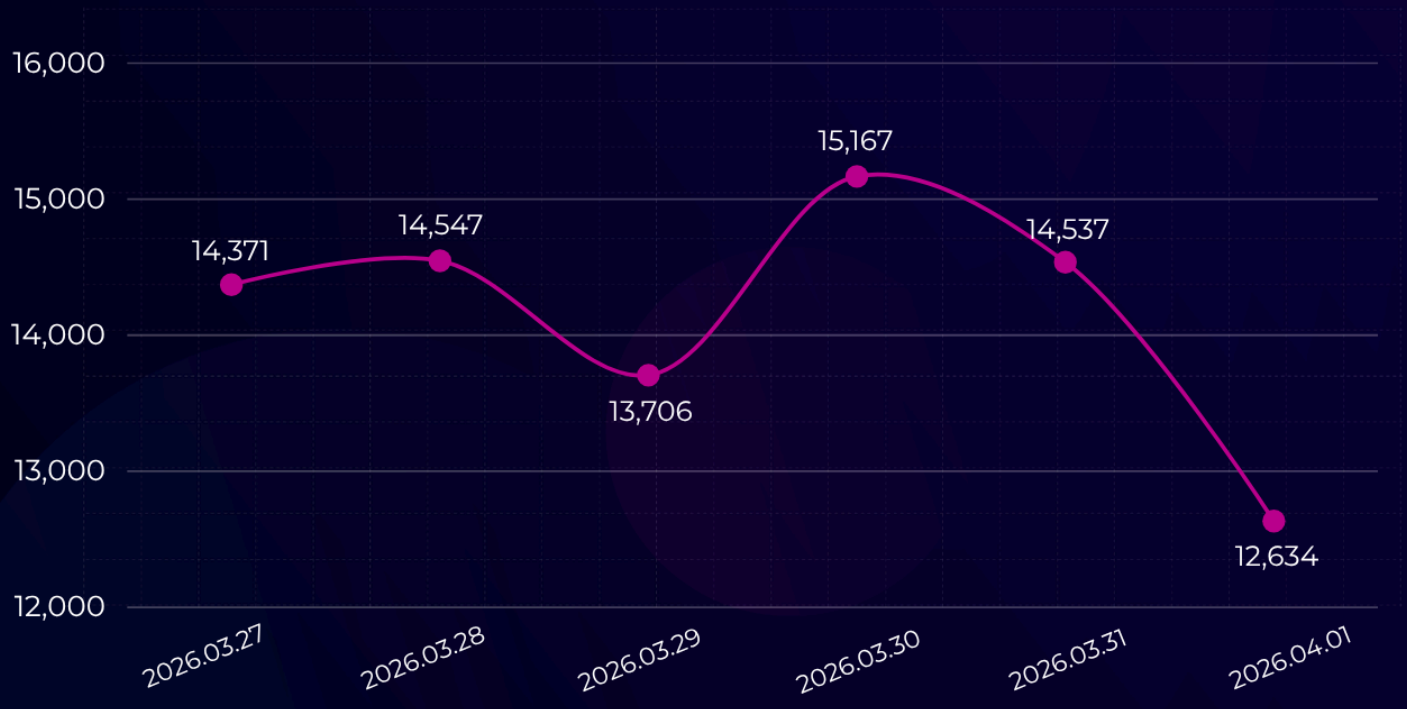
Тоон мэдээлэл нь IP хаягийн давхардлыг арилгасан мэдээлэлд суурилсан болно.



Халдлага, зөрчлийн ангилал

Эмзэг байдалтай сүлжээний сервис:	2622	Халдлага (brute-force гэх мэт) :	68
Эмзэг байдалтай файл шэйрлэлт :	1114	Блоклогдсон IP хаяг:	66
Сүлжээний урсгал өөрчлөлт :	587	Эзлэгдсэн IoT төхөөрөмж:	19
Эмзэг байдалтай вэб сайт:	558	Интернэтэд тавигдсан хорт программ:	5
Scanner (эмзэг байдал гэх мэт) :	81		

Нийт халдлага, зөрчлийн тоо (өдрөөр)



ХАМТЫН АЖИЛЛАГААНЫ САНАМЖ БИЧИГТ ГАРЫН ҮСЭГ ЗУРЛАА

“Кибер халдлага, зөрчилтэй тэмцэх нийтийн төв” УТҮГ болон Кибер халдлага, зөрчилтэй тэмцэх Зэвсэгт хүчний төв хамтын ажиллагааны санамж бичигт гарын үсэг зурлаа.

Энэхүү санамж бичгийн хүрээнд талууд кибер орчинд үйлдэгдэж буй халдлага, зөрчлийг илрүүлэх, таслан зогсоох, урьдчилан сэргийлэх чиглэлээр хамтран ажиллах, холбогдох хууль тогтоомжийн хүрээнд мэдээлэл солилцох, харилцан сургалт зохион байгуулах, мэргэжил, арга зүйн дэмжлэг үзүүлэхээр тохиролцов.

Хамтын ажиллагааны хүрээнд 2026.02.25-ны өдөр Төв аймгийн Заамар суманд нийт 237 төрийн албан хаагчид, ахлах ангийн сурагчид болон ПТК-ийн оюутнуудад мэдээллийн аюулгүй байдал, цахим орчинд хувийн мэдээллээ хамгаалах сэдвээр сургалт зохион байгууллаа.

ОЛОН УЛСЫН ХАМТЫН АЖИЛЛАГАА

КИБЕР ХАЛДЛАГА, ЗӨРЧИЛТЭЙ ТЭМЦЭХ НИЙТИЙН ТӨВ

APCERT
Asia Pacific Computer Emergency Response Team

“Кибер халдлага, зөрчилтэй тэмцэх нийтийн төв” УТҮГ 2025 оны 8 дугаар сард Ази, Номхон далайн бүсийн орнуудын кибер халдлагад хариу үзүүлэх багуудын хамтын ажиллагааны байгууллага болох **APCERT**-ийн албан ёсны гишүүнээр элсэж, гишүүний хувиар 2025 оны жилийн тайланд нь тусгагдлаа.

Гишүүн болсноор олон улсын кибер халдлагын мэдээллийг шуурхай солилцох, хариу арга хэмжээний чадавхаа бэхжүүлэх, гишүүн байгууллагуудтай хамтын ажиллагаагаа өргөжүүлэх, мэргэжлийн ур чадвараа хөгжүүлэх боломж бүрдэж байна.

Энэ нь Монгол Улсын кибер аюулгүй байдлын салбарын олон улсын оролцоо, хамтын ажиллагааг шинэ түвшинд хүргэсэн чухал алхам юм.

ANNUAL REPORT 2025

QR кодыг уншуулан тайлантай танилцана уу.

КИБЕР АЮУЛГҮЙ БАЙДЛЫН СУРГАЛТ ЗОХИОН БАЙГУУЛАГДЛАА

Нийтийн төвийн үйл ажиллагааны нэг чиглэл болох **“Сургалт зохион байгуулах”**-ын хүрээнд иргэн, байгууллагуудын кибер аюулгүй байдлын мэдлэг, ур чадварыг дээшлүүлэх сургалтуудыг тогтмол зохион байгуулж байна.

2026.02.04

“Кибер халдлага, зөрчилтэй тэмцэх нийтийн төв” УТҮГ нь Нийслэлийн Эрүүл мэндийн газартай хамтран эрүүл мэндийн салбарын 28 байгууллагын удирдлага болон мэдээллийн аюулгүй байдлын хариуцсан мэргэжилтнүүдэд зориулсан кибер аюулгүй байдлын сургалт зохион байгууллаа.

Кибер аюулгүй байдлын хууль, эрх зүйн орчин, халдлагад хариу үзүүлэх арга хэмжээ, урьдчилан сэргийлэх арга замын талаар онол, практик мэдлэг олгов.

2026.02.26

“Cybersecurity Awareness Program”-ын хүрээнд Olula сургуулийн 100 гаруй сурагчдад мэдээллийн аюулгүй байдлын сургалт зохион байгууллаа.

Цахим орчны эрсдэл, нууц үгийн аюулгүй байдал, хоёр шатлалт баталгаажуулалт (2FA), цахим дээрэлхэлтээс урьдчилан сэргийлэх арга замын талаар ойлголт өгч, цахим орчинд өөрийгөө хамгаалах зөв дадлыг төлөвшүүлэхэд чиглэсэн мэдлэг мэдээлэл хүргэлээ.

2026.05.20

Мэдээллийн технологийн үндэсний паркийн инкубатор компаниудын дунд сургалт зохион байгууллаа.

Оролцогчдын хэрэгцээ, сонирхолд үндэслэн мэдээллийн аюулгүй байдлын суурь ойлголт, кибер халдлагаас урьдчилан сэргийлэх арга зам, эрсдэлийн удирдлага болон байгууллагын өөгдөл хамгаалалтын талаар практик мэдлэг, мэдээллийг хүргэлээ.

ЯРИЛЦЛАГЫН БУЛАН

Мэдээллийн аюулгүй байдлын аудитор Б.Дашдорж

Батмөнхийн Дашдорж нь Кибер халдлага, зөрчилтэй тэмцэх нийтийн төв УТҮГ-т 2024 оноос ажиллаж эхэлсэн бөгөөд одоогоор Мэдээллийн аюулгүй байдлын аудиторын албан тушаалыг хашиж байна. Тэрээр өмнө нь тус нийтийн төвийн 113 тусгай дугаар, 113.mn сайт болон иргэн, хуулийн этгээдээс кибер халдлага, зөрчлийн мэдээлэл хүлээн авах, дүн шинжилгээ хийх, иргэн байгууллагад зөвлөмж хүргэх чиглэлээр ажиллаж байсан туршлагатай.

Өдөр бүр өөр, гэхдээ нэг зорилготой

Ажлын өдрөө тэрээр өмнөх шөнийн бүртгэгдсэн тохиолдол, системийн анхааруулга (alert), мэдээллүүдийг шалган эхлүүлдэг. Кибер аюулгүй байдлын салбарт эрсдэл ямар ч үед үүсэж болдог тул тасралтгүй хяналт хамгийн чухал байдгийг онцоллоо.

Өдөр тутмын ажил нь иргэд, байгууллагуудаас ирсэн мэдээллийг ангилан үнэлэхээс эхлээд эрсдэлийн түвшин тогтоох, зөвлөгөө өгөх, шаардлагатай тохиолдолд шуурхай арга хэмжээ авах хүртэл өргөн хүрээг хамардаг. Харин одоо аудитын чиглэлээр ажиллаж байгаа тул байгууллагуудын мэдээллийн аюулгүй байдлын бодлого, эрсдэлийн удирдлага, ISO 27001 стандартын хэрэгжилт, дотоод хяналт, аудитын үнэлгээнд түлхүү анхаарч байна.

Хуурамч линк, залилангийн мэдээлэл хамгийн олон бүртгэгддэг

Сүүлийн жилүүдэд иргэдийн хамгийн түгээмэл тулгарч буй асуудал нь фишинг халдлага, хуурамч вебсайт, сошиал хаяг алдагдах, онлайн залилан болон банкны мэдээлэлтэй холбоотой сэжигтэй тохиолдлууд болжээ. Зарим иргэн хохирол амссаны дараа ханддаг бол зарим нь эрсдэлээс урьдчилан сэргийлэх зорилгоор зөвлөгөө авдаг байна.

Хүний хүчин зүйл хамгийн том эрсдэл

Түүний ажилласан олон тохиолдолд байгууллагын нэрийг дуурайсан хуурамч вебсайт, нэвтрэх систем ашиглан мэдээлэл авах оролдлого түгээмэл байдаг. Ийм халдлагууд нь ихэвчлэн техникийн сул талыг бус, хүний итгэлцэл, яаруу шийдвэр гаргах хандлагыг ашигладаг онцлогтой гэв.

Өнөөдөр кибер аюулгүй байдал бол зөвхөн мэргэжилтнүүдийн асуудал биш, хүн бүрийн өдөр тутмын амьдралын нэг хэсэг болсон.

Тасралтгүй суралцах шаардлагатай салбар

Кибер аюулгүй байдлын салбарын хамгийн сонирхолтой тал нь байнга хувьсаж, шинэ сорилтууд гарч ирдэгт оршдог. Үүний зэрэгцээ цаг хугацаатай уралдан зөв үнэлгээ хийж, шуурхай шийдвэр гаргах шаардлага байнга тулгардаг.

Б.Дашдорж өөрийгөө хөгжүүлэхийн тулд олон улсын кибер аюулгүй байдлын мэдээ, судалгаа, threat intelligence мэдээллийг тогтмол уншиж, лабораторийн орчинд шинэ технологи туршин, аудит болон засаглалын чиглэлийн мэдлэгээ тасралтгүй ахиулдаг байна.

Залуу мэргэжилтнүүдэд өгөх зөвлөгөө

Тэрээр энэ салбарт ажиллахыг хүсэж буй залууст сүлжээ, үйлдлийн систем, системийн удирдлага зэрэг суурь мэдлэгээ сайн эзэмшихийг зөвлөж байна. Мөн зөвхөн диплом бус бодит практик туршлага, тасралтгүй суралцах хандлага хамгийн том давуу тал болдог гэдгийг онцоллоо.

“Кибер аюулгүй байдал бол зөвхөн мэргэжлийн хүмүүсийн асуудал биш. Өнөөдөр хүн бүрийн өдөр тутмын амьдралтай холбоотой болсон учраас байгууллага, иргэн бүр мэдээллийн аюулгүй байдлын мэдлэгээ нэмэгдүүлж, эрсдэлээс урьдчилан сэргийлэх соёлыг хэвшүүлэх нь хамгийн чухал” хэмээн тэрээр ярилцлагын төгсгөлд хэллээ.

ОХИДЫН АЮУЛГҮЙ БАЙДЛЫГ КИБЕР ОРЧИНД Ч ХАМГААЛЪЯ

Өсвөр насны охидыг цахим орчин дахь гэмт хэрэг, хүчирхийллээс урьдчилан сэргийлэхэд дүүрэг, хороо, ерөнхий боловсролын сургуулийн нийгмийн ажилтан, сэтгэл зүйчдийн мэдлэг, чадавхыг бэхжүүлэх зорилгоор тус Нийтийн төвөөс **“CyberSafe Girls” үндэсний аяныг** санаачлан хэрэгжүүлж байна.

Харилцаа холбооны зохицуулах хороо

Кибер гэмт хэрэгтэй тэмцэх газар

Тус аяныг Харилцаа холбооны зохицуулах хороо, Цагдаагийн ерөнхий газрын Кибер гэмт хэрэгтэй тэмцэх газартай хамтран охидын цахим аюулгүй байдлыг хамгаалах чиглэлээр мэдлэг, мэдээлэл түгээж байна.

ЗОХИОН БАЙГУУЛСАН СУРГАЛТУУД

2025.11.03

Баянзүрх дүүргийн ИТХ, Гэмт хэргээс урьдчилан сэргийлэх ажлыг зохицуулах салбар зөвлөл, Эмэгтэйчүүдийн зөвлөлтэй хамтран 43 хорооны хамтарсан багийн гишүүдэд сургалт зохион байгууллаа.

2026.06.04

Хан-Уул дүүргийн ИТХ-тай хамтран ерөнхий боловсролын 24 сургуулийн нийгмийн ажилтан, сэтгэл зүйчдийг хамруулсан сургалт амжилттай зохион байгууллаа.

2026.06.17

Чингэлтэй дүүргийн 24 хорооны 60 нийгмийн ажилтан болон гэмт хэргээс урьдчилан сэргийлэх ажлыг зохицуулах салбар зөвлөлийн гишүүдийн дунд сургалт зохион байгууллаа.

ХӨТӨЛБӨРИЙН ХҮРЭЭНД

- Цахим орчин дахь охид, эмэгтэйчүүдийн эсрэг хүчирхийлэл
- Цахим орчин дахь хүүхэд хамгаалал
- Охидод чиглэсэн кибер гэмт хэргийн бодит кейсүүд ба хууль эрх зүйн орчин
- Сошиал медиа платформууд ба охидын аюулгүй байдал

сэдвүүдээр сургалт явуулан, хэлэлцүүлэг өрнүүлж, оролцогчдын мэдлэг, ойлголтыг нэмэгдүүллээ.

“Цахим орчин дахь охидын аюулгүй байдлыг хангахад зөвхөн хууль эрх зүйн зохицуулалт, технологийн шийдэл хангалтгүй юм. Эцэг эх, багш сурган хүмүүжүүлэгчид, нийгмийн ажилтнуудын хамтын оролцоо нэн чухал юм.

CYBERSAFE GIRLS 2026
Stay Smart, Stay Safe

WOMEN in TECH®

“CyberSafe Girls” аян нь WomenTech Mongolia 2026 арга хэмжээний үеэр “**Шилдэг дэмжигч**” шагнал хүртлээ.

“CyberSafe Girls” аян нь өсвөр насны охидыг кибер халдлага, цахим орчинд үйлдэгддэг гэмт хэрэг, зөрчлөөс урьдчилан сэргийлэхэд нийгмийн ажилтнуудын оролцоог нэмэгдүүлж, мэдлэг, чадавхыг бэхжүүлэхэд чиглэж байна. Цаашид энэхүү санаачилгыг 21 аймаг, 9 дүүрэгт хэрэгжүүлж, охидын аюулгүй байдлыг хамгаалах тогтолцоог улам бүр бэхжүүлэхээр зорин ажиллаж байна.

Кибер дипломат ажиллагаа: Дижитал шилжилтийн эрин дэх олон улсын харилцааны хөгжил, сорилт ба боломжууд

Гантөмөрийн Гантуяа
Докторант, Кибер халдлагаас урьдчилан сэргийлэх газрын дарга, Кибер халдлага, зөрчилтэй тэмцэх нийтийн төв

Хаш-Эрдэнийн Урангоо
Доктор, Эрдэм шинжилгээний ахлах ажилтан, Монгол Улсын Аюулгүй байдал судлалын хүрээлэн

Даваадашийн Дүгэрсүрэн
Эрдэм шинжилгээний ахлах ажилтан, Монгол Улсын Аюулгүй байдал судлалын хүрээлэн

Энэхүү өгүүлэлд дижитал шилжилтийн эрин үед олон улсын харилцааны шинээр төлөвшин буй чиглэл болох кибер дипломат ажиллагааны онолын болон практик үндсийг авч үзэв. Судалгаанд кибер дипломат ажиллагааны үндсэн чиглэлүүдийг тодорхойлж, үүнд олон улсын кибер аюулгүй байдлыг хангах (кибер орчин дахь итгэлцэл бэхжүүлэх арга хэмжээ (CBMs), бүх нийтээр хүлээн зөвшөөрсөн хэм хэмжээ (norms), институцчилсэн хамтын ажиллагааны механизм), кибер орчин дахь олон улсын эрх зүйн хэм хэмжээг төлөвшүүлэх, улс орнуудын дижитал орчин дахь үндэсний чадавхыг бэхжүүлэх асуудлыг онол, практикийн хүрээнд шинжилсэн.

Түүнчлэн кибер дипломат ажиллагааг институцчлах үйл явцад United Nations (НҮБ), Budapest Convention on Cybercrime болон бүс нутгийн хамтын ажиллагааны санаачилгуудын гүйцэтгэх үүрэг, ач холбогдлыг шинжилсэн. Эдгээр олон улсын механизм нь кибер орчин дахь төрийн хариуцлагатай оролцоо, хамтын ажиллагааны зарчим, эрх зүйн зохицуулалтыг төлөвшүүлэхэд чухал үүрэгтэй болохыг харуулж байна.

QR уншуулж судалгааны өгүүллийг уншина уу

Монгол Улсыг жишээ болгон авч үзэхдээ үндэсний кибер аюулгүй байдлын өнөөгийн нөхцөл байдал, холбогдох хууль эрх зүйн орчин, кибер халдлага, зөрчилтэй тэмцэх төвүүд (CERT/CSIRT)-ийн үйл ажиллагаа, олон улсын хамтын ажиллагаанд оролцож буй түвшинд дүн шинжилгээ хийв. Судалгаанд International Telecommunication Union (ITU) болон Global Cybersecurity Capacity Centre (GCSCC)-ийн тайлан, үнэлгээний үр дүнг ашигласан бөгөөд эдгээр нь Монгол Улс хууль эрх зүй, байгууллагын тогтолцооны хувьд тодорхой ахиц гаргаж буйг харуулж байна. Ялангуяа кибер аюулгүй байдлын үндэсний бодлого, зохицуулалтын орчин бүрэлдэн тогтож, байгууллагын бүтэц, зохион байгуулалтын чадавх сайжирч буй нь эерэг үзүүлэлт гэж үнэлэгдэв.

Гэвч техник, технологийн чадавх, дэд бүтэц, мэргэжлийн хүний нөөцийн хүрэлцээ, түүнчлэн олон улсын хамтын ажиллагааг өргөжүүлэх чиглэлээр тодорхой сорилтууд тулгарсаар байна. Тухайлбал, кибер халдлагыг илрүүлэх, урьдчилан сэргийлэх, хариу арга хэмжээ авах техникийн чадавхыг бэхжүүлэх, мөн олон улсын түвшний мэдээлэл солилцоо, хамтарсан ажиллагаанд оролцох боломжийг өргөжүүлэх шаардлага хэвээр байна.

Судалгааны үр дүнгээс үзэхэд кибер дипломат ажиллагаа нь орчин үеийн олон улсын харилцааны салшгүй бүрэлдэхүүн хэсэг болж, дэлхийн тогтвортой байдал, кибер орчны аюулгүй байдал, төрийн хариуцлагатай оролцоог хангах чухал хэрэгсэл болон төлөвшиж байна. Иймд Монгол Улсын хувьд кибер дипломат ажиллагааг цаашид үр дүнтэй хөгжүүлэхэд мэргэшсэн хүний нөөцийг бэлтгэхийн зэрэгцээ холбогдох байгууллагуудын уялдаа холбоог бэхжүүлэх, гадаад харилцааны бодлого, үйл ажиллагаатай уялдуулан институцийн оролцоог хангах, олон улсын эрх зүйн санаачилга, хамтын ажиллагаанд идэвхтэй, тогтвортой оролцох нь тэргүүлэх чиглэл болохыг дүгнэв.

Кибер халдлагаас урьдчилан сэргийлэх 10 зөвлөмж

Хүчтэй нууц үг ашиглах

Том, жижиг үсэг, тоо, тусгай тэмдэгт хослуулсан 12-аас дээш тэмдэгттэй нууц үг хэрэглэ.

Цахим залилан, хуурамч зар сурталчилгааг нягтал

Хэт ашигтай санал, сугалаа, мөнгөний амлалтууд нь ихэвчлэн залилан байдаг.

Хоёр шатлалт баталгаажуулалт (2FA) идэвхжүүлэх

Facebook, мэйл, банкны апп зэрэг бүх чухал платформдоо ашиглах.

Эх сурвалжийг шалга

Мэдээлэл уншихдаа вебсайтын хаяг, байгууллагын нэр, албан ёсны эх сурвалж мөн эсэхийг нягтал.

Сэжигтэй холбоос дээр бүү дар

“Шагнал хожлоо”, “Дансаа баталгаажуул” гэх мэт яаруулсан мессеж, холбоос нь хуурамч байх эрсдэлтэй.

Үйлдлийн систем, аппликейшнээ тогтмол шинэчлэх

Шинэчлэлт бүр системд гарсан аюулгүй байдлын цоорхойг нөхөж байдаг.

Хувийн мэдээллээ хамгаалах

Регистрийн дугаар, картын дугаар, пин код, OTP код, нууц үгээ хэнд ч битгий хэл.

Мэдээллээ нөөцлөх

Зураг, баримт бичиг, ажлын файлуудаа төхөөрөмж эсвэл үүлэн санд хадгалж хэвших.

Цахим орчинд хэт их мэдээлэл бүү нийтэл

Байршил, утасны дугаар, гэр бүлийн зураг зэрэг хувийн мэдээллээ хуваалцахаас зайлсхий.

Үнэгүй WIFI ашиглахдаа болгоомжлох

Олон нийтийн wifi ашиглахдаа банкны гүйлгээ, нууц үг оруулах, чухал мэдээллээ дамжуулахгүй байх.

Халдагчид таны төхөөрөмж биш сэтгэлзүй рүү халддаг.

PUBLIC CSIRT/CC

КИБЕР ХАЛДЛАГА МЭДЭЭЛЭХ

113

113.mn

Pubcert.mn

GOVERNMENT PARTNER

OffSec

OPERATIONAL MEMBER OF:

APCERT

FIRST

ХАЯГ:

Баянгол дүүрэг, 17-р хороо, Амарсанаагийн гудамж, Радио телевизийн үндэсний сүлжээ УТУГ-ын байр, 2 давхарт, Улаанбаатар хот, Монгол улс, 15160

И-МЭЙЛ:

contact@pubcert.mn