**COURSE: INTRODUCTION TO INFORMATION SYSTEM**

**Lecture 15 - Security and Ethical Challenges of e-Businessy**

**Lecturer:**

**SARANCHIMEG Nasanjargal**

## Судлах зүйлс

Бизнест мэдээллийн технологиудыг ашиглах нь ажил эрхлэлт, хувийн хүний онцлог шинж, ажлын нөхцөл, хувийн хэрэг, гэмт хэрэг, эрүүл мэнд болон нийгмийн асуудлуудын шийдлүүдэд хэрхэн нөлөөлж байгаатай холбоотой ёс суртахууны анхаарал татсан асуудлуудыг тодорхойлох.

Аюулгүй байдлын удирдлагын стратегиуд ба хамгаалалтын төрлүүдийг тодорхойлж, тэдгээрийг мэдээллийн технологийн бизнесийн хэрэглээний програмуудын аюулгүй байдлыг баталгаажуулахад хэрхэн ашиглаж болохыг тайлбарлах.

# МТ-ИЙН ХАМГААЛАЛТ, ЁС СУРТАХУУН БА НИЙГЭМ

### *Мэдээлэл бол хөрөнгө*

Мэдээллийг оюун ухааны үйл ажиллагааны үр дүн гэж тодорхойлдог. Энэ нь мэдээллийн хэрэгслээр дамжуулагддаг биет бус бүтээгдэхүүн юм. Ерөнхийдөө мэдээлэл бол өгөгдлийн боловсруулалт, ашиглалт, зохион байгуулалтын үр дүн ба энгийнээр бол баримтын цуглуулга хэмээн тодорхойлсон байдаг.

Мэдээллийн аюулгүй байдлын салбарт мэдээллийг “хөрөнгө” гэж тодорхойлдог. Энэ нь үнэ цэнэ бүхий зүйл учраас хамгаалагдах ёстой зүйл юм. Мэдээлэлд өгч буй ач холбогдол нь өнөөдөр хөдөө аж ахуйн нийгмээс аж үйлдвэрийн нийгэм рүү, эцэст нь мэдээлэлд чиглэсэн нийгэм рүү шилжих шилжилтийг харуулдаг.Хөдөө аж ахуйн нийгэмд газар хамгийн чухал хөрөнгө байсан бөгөөд буудайн хамгийн том үйлдвэрлэлтэй орон өрсөлдөх чадвартай байдаг байв. Аж үйлдвэрийн нийгэмд газрын тосны нөөцтэй байх гэх мэт хөрөнгийн бат бэх байдал өрсөлдөх чадварын гол хүчин зүйл нь байсан. Мэдлэг, мэдээлэлд суурилсан нийгэмд, мэдээлэл нь хамгийн чухал хөрөнгө бөгөөд мэдээлэл цуглуулж, дүн шинжилгээ хийж ашиглах чадвар нь ямар ч улсын өрсөлдөх чадварыг илэрхийлэх давуу тал юм. Хүмүүсийн үзэл санаа бодит хөрөнгийн үнэ цэнээс мэдээллийн хөрөнгийн үнэлэмж рүү шилжихийн хэрээр мэдээллийг хамгаалах ёстой гэсэн үзэл санаа улам бүр гүнзгийрч байна. Мэдээлэл нь өөрөө түүнийг агуулж буй хэвлэл, мэдээллийн хэрэгслээс илүү үнэлэгддэг

### *Мэдээллийн аюулгүй байдал гэж юу вэ?*

Мэдээллийг хууль бусаар олж авах оролдлогын хариуд хүмүүс мэдээлэлтэй холбоотой гэмт хэргээс сэргийлэх эсвэл ийм төрлийн гэмт хэргийн учруулах хохирлыг багасгахад идэвхи чармайлт гаргаж байна. Энгийнээр хэлбэл, **мэдээллийн аюулгүй байдал бол** мэдээллийн үнэ цэнийг таньж түүнийг хамгаалах явдал юм.

**Мэдээллийн аюулгүй байдлын 4R**

Мэдээллийн аюулгүй байдлын 4R гэдэг бол зөв мэдээлэл (Right information), зөв хүмүүс (Right people), зөв цаг (Right time), зөв хэлбэр (Right form) юм. 4R-ыг хянах нь мэдээллийн үнэ цэнийг хадгалан, хянах хамгийн үр дүнтэй арга юм. Мэдээллийн аюулгүй байдлыг хамгаалахын тулд 4R-ыг зөв ашиглах ёстой. Энэ нь мэдээлэлтэй харьцах үедээ нууцлал, нэгдмэл болон боломжит байдлыг дагаж мөрдөх ёстой гэсэн үг юм. Мэдээллийн аюулгүй байдал нь мэдээллийн хөрөнгийн үнэ цэнэ, тэрчлэн тэдгээрийн эрсдэлд эмзэг байдал ба холбогдох аюул заналын талаар тодорхой ойлгосон байхыг шаарддаг.


**Зураг 0-1. Мэдээллийн аюулгүй байдлын 4R**

### *Компьютерийн гэмт хэрэг*

Техник хангамж, Программ хангамж, өгөгдөл ба сүлжээний нөөцүүдийг зөвшөөрөлгүй ашиглах, хандах, засаж өөрчлөх, сүйтгэх мэдээллийг зөвшөөрөлгүй нийтэд мэдээллэх Программ хангамжийг зөвшөөрөлгүй хуулбарлах эцсийн хэрэглэгчийг өөрийнх нь техник хангамж, Программ хангамж, өгөгдөл эсвэл сүлжээний нөөцүүд рүү хандуулахгүй байх Мэдээллийг эсвэл бодит тодорхой өмчийг олж авахад компьютер ба сүлжээний нөөцүүдийг хууль бусаар ашиглах, хуйвалдах зэрэг орно. **Кибер хулгай** гэдэг нь голдуу ажлын байранд эсвэл интернетийг хэрэглэн мөнгө хулгайлах үйлдлийг агуулсан компьютерийн гэмт хэрэг юм. **Ажил дээрх зөвшөөрөлгүй ашиглалт** гэдэг нь компьютерийн системийн болон сүлжээний зөвшөөрөлгүй ашиглалт буюу *цаг хугацааны ба нөөцийн хулгай* гэнэ. Хувираа зөвлөлгөө өгөх эсвэл өөрийгөө санхүүжүүлэх, эсвэл видео тоглоом тоглох, компаний сүлжээн дээр интернетийг зөвшөөрөлгүй ашиглах гэх мэт янз бүрийн хэлбэртэй байж болно. Ажлын байран дээрх интернетийн зүй бус ашиглалтанд:

- И-мэйлийн буруу ашиглалт
- Зөвшөөрөлгүй ашиглалт ба хандалт
- Newsgroup-ийн мэдээнүүд
- Нууц өгөгдлийг дамжуулах
- Садар самуун – сексийг ил тод харуулсан сайтууд руу хандах
- Хакердах
- Ажилтай холбоогүй мэдээллийг татан авах эсвэл ачааллах
- Интернетийг чөлөөтэй, зугаа цэнгэлийн зорилгоор ашиглах
- Гадны ИҮТ (ISP)-ийг ашиглах
- Үндсэн ажлаас гадуур ажил эрхлэх
- Зохиогчийн эрхийг зөрчих/зохиолын хулгай -

### *Халдлага (Hacking)*

**Халдлага** гэж сүлжээгээр холбогдсон компьютерийн сүлжээнд зөвшөөрөлгүй хандах ба ашиглах буюу мэдээлэл авах, өөрчлөхийн тулд компьютер болон компьютерийн сүлжээнд албан ёсны зөвшөөрөлгүйгээр нэвтрэхийг хэлнэ. Халдлагын зорилгоос хамаарч **зугаацлын, гэмт хэргийн болон улс төрийн** гэж ангилдаг. Зугаацлын шинжтэй халдлага нь тухайн хууль бусаар нэвтрэгч этгээд сониуч зан авирын улмаас програм болон өгөгдлийг зөвшөөрөлгүй өөрчлөх ажиллагаа юм. Гэмт хэргийн шинжтэй халдлагыг залилан болон тагнуулын зорилгоор ашигладаг. Улс төрийн хууль халдлага гэж зөвшөөрөлгүй улс төрийн мэдээ, мэдээллийг цацахын тулд вебсайт руу нэвтрэхийг хэлнэ. Сүүлийн үед халдлага нь кибер заналхийлэл ба кибер дайны нэг хэсэг болох нь улам бүр ихэсч энэ нь үндэсний аюулгүй байдалд ихээхэн аюулыг учруулж байна. Вирус болон worm (өт)-ууд нь сүлжээгээр холбогдсон компьютеруудад төвөг учруулсан эсвэл эвдэн сүйтгэсэн тусгай програмыг хуулах бөгөөд голдуу имэйлээр эсвэл интернетээр дамжуулж буй файлуудаар тархдаг. Компьютерийн **вирус** нь өөр программ руу нэвтрэн орохгүй бол ажиллаж чаддаггүй програмын код бол **Worm** (Өт) нь ямар нэгэн програмын тусламжгүйгээр ажиллаж чаддаг эвдэн сүйтгэгч програм юм.

**Adware -** Компьютер дээр програмыг суулгасаны дараа эсвэл хэрэглээний програмыг хэрэглэж байх үед хэрэглэгч тухайн програмыг ажиллуулаагүй, хүсээгүй байхад сурталчилгааны материалыг автоматаар тоглуулж, харуулж эсвэл татаж авдаг програм. Адвэйр бол үнэгүй программ, тоглоом, элдэв хэрэгслүүдийг дагалдан тараагддаг жижиг код

юм. Энэхүү жижигхэн кодийн зориулалт нь үнэгүй программ хийсэн компани болон тэрхүү компанийн түншүүдийн сурталчилгааг тодорхой заасан хугацаагаар хэрэглэгчдэд хүргэхэд оршдог. Зарим тохиолдолд уг үнэгүй программыг тодорхой төлбөр төлөн бүртгүүлснээс хойш уг программын адвэйр ажиллахгүй идэвхгүй болдог. Товчхондоо бол адвэйр нь программ хангамжийг дагалдан ирдэг сурталчилгааны жижигхэн код гэж ойлгож болох юм. (Б.Батхишиг, Д.Чинзориг, Энхбилгүүн, Пагамноржин, Мөнхшүр, 2012)

**Spyware -** Хэрэглэгчийн зөвшөөрөлгүй эсвэл мэдээгүй байхад хэрэглэгчийн интернетийн холболтыг нууцаар ашиглан хэрэглэгчийн тухай мэдээллийг цуглуулж, түүнийг интернетээр илгээж байдаг Adware программын хууль бус хэлбэр юм. Хэрэглэгчийн нүүр хуудсыг өөрчлөн, үзэж байгаа зүйлийг чиглүүлэн хэрэглэгчийн браузерыг хүчээр өөр чиглэл рүү оруулж чаддаг. **OPT-IN (Дэмжих)** - Имэйлийн листэнд нь бүртгүүлэх замаар тодорхой компаниас, бүлэг компаниас эсвэл холбоотой компаниас имэйлүүд хүлээн авахыг зөвшөөрсөн үйлдэл.

**OPT-OUT (Татгалзах)** - Захиалга хийгээгүй хүмүүс рүү имэйлүүд явуулж, тэднийг жагсаалтаас гадна байлгах боломж олгодог мэйлийн лист. Захиалагчдын имэйл хаягуудыг вэбээс, USENET, эсвэл мэйлийн жагсаалтуудаас олж авна. ISP-ийн бодлогууд болон зарим мужийн хуулиудаар хориглож болно.

**ХЯТАД, АМЕРИКИЙН СҮЛЖЭЭНИЙ ДАЙН**

Америкийн Нэгдсэн улсад (АНУ) төвтэй ПойзонБокс гэх хакерын бүлэг Хятадын 350 гаруй сайтуудын үйл ажиллагааг сарын турш доголдуулсан хэргээр буруутгагдсан. Тус бүлэг нь Хятадын төрийн найман байгууллагын вебсайтад 2001 оны 4 сарын 30-нд халдсан гээд хэдийнээ Хятадын 24 вебсайт руу халдчихаад байв. Үүний дараа Хятадын хакерууд Үндэсний батлан хамгаалахын төлөөх зургаа дахь удаагийн сүлжээний дайныг зарлаж 2001 оны 4 сарын 30-наас 5 сарын 1-ны хооронд АНУ-ийн засгийн газрын байгууллагуудын вебсайтууд гэх мэт АНУ-д төвтэй сайтууд руу халдсан байна. Халдлагууд нь Пентагоныг компьютерийн системийн хамгаалалтын төвшнөө INFO-CON NORMAL-аас INFO-CON ALPHA руу өсгөхөд хүргэв. 2001 оны 5 сарын 1-ны өдөр Холбооны мөрдөх товчооны Үндэсний дэд бүтцийн хамгаалалтын төвөөс Хятадын хакерууд АНУ-ын засгийн газрын болон компанийн веб сайтууд руу дайралт хийж буй талаар анхааруулга гаргасан байна. Сүлжээний дайны дараагаар АНУ цахим заналхийлэл (хууль бус нэвтрэлт зэрэг) нь АНУ-ын засгийн газрын байгууллагуудад маш их хохирол учруулах чадвартай гэдгийг хүлээн зөвшөөрсөн бөгөөд үүний дараагаар мэдээллийн аюулгүй байдлын төсөв болон засгийн газрын байгууллагуудын доторх мэдээллийн бодлогыг сайжруулах зэрээр кибер заналхийлэлийн эсрэг хамгаалалтыг нэмэгдүүлсэн байна.

*Эх сурвалж: Attrition.org, "Cyberwar with China: Self*

### *Хакерын нийтлэг тактикууд*

1. **Үйлчилгээг бусниулах довтолгоо (Denial-of-Service)**

Үйлчилгээг бусниулах довтолгоо- УБ (Denial of Service) зэрэг халдлагууд нь хууль бус нэвтрэгч машин болон өгөгдөл рүү зөвшөөрөлгүйгээр нэвтэрч байхад хууль ёсны хэрэглэгчид үйлчилгээг ашиглах боломжгүй байдаг. Энэ нь халдлага үйлдэгчид сүлжээг их хэмжээний өгөгдлөөр "ачаалж" эсвэл процесс хяналтын хаалт, хүлээгдэж буй сүлжээний холболт гэх мэт хязгаарлагдмал нөөцийг зориудаар ашиглах зэргээр үйлдэгдэнэ. Эсвэл тэд

сүлжээний бүрдэл хэсгийг тасалдуулах болон цоожлогдсон өгөгдөл гэх мэт шилжилтийн шатанд байгаа өгөгдлийг ашигладаг.

**ЭСТОНИЙН ЭСРЭГ КИБЕР ЗАНАЛХИЙЛЭЛ**

2007 оны 5 сарын 4-нд Эстонийн нийслэл хотод, ЗХУ-ын ялалтын хөшөөг хотын төвөөс цэргийн оршуулгын газар луу шилжүүлсэнээс үүдэн Эстоний эсрэг гурван долоо хоног үргэлжилсэн кибер халдлага гарсан бөгөөд сая сая компьютеруудад үйлчилгээг бусниулах довтолгоо (DoS) гэх мэт халдлагуудыг хийсэн байна. Ерөнхийлөгчийн ордон, Эстонийн парламент, эрх баригч нам,хэвлэл мэдээллийнхэн болон банкуудын компьютерийн сүлжээ, вебсайтууд доголдсон байна. Тэр бүү хэл утасгүй сүлжээ хүртэл халдлагад өртсөн байна. Хожим нь халдлага үйлдэгчийн байршил нь Оросын засгийн газрын байгууллага байсныг олж тогтоосон юм. Харин Оросын засгийн газар үүнийг няцаасан байна. Халдлагын эсрэг баг болон мэдээллийн аюулгүй байдлын бодлого дутмагийн улмаас Эстони тэрхүү кибер халдлага гарсан даруйд хариу арга хэмжээ авах боломжгүй байсан.

*Эх сурвалж: Beatrix Toth, "Estonia under cyber attack" (Hun-CERT, 2007), http://www.cert.hu/dmdocuments/Estonia_attack2.pdf*

**2. Хортой код (Malicious code)**

Хортой код гэж ажилласан тохиолдолд системд гэмтэл учруулдаг програмыг хэлдэг. Вирус, өт, трояны морь зэрэг нь хортой кодын төрлүүд юм.

Компьютерийн вирус гэдэг нь өөр програм, компьютерийн асах хэсэг эсвэл баримт бичигт өөрийн хувилбарыг үүсгэн олширч компьютерийн систем болон өгөгдлийг гэмтээдэг компьютерийн програм болон програмчилалын код юм.

Компьютерийн өт нь файлуудыг өөрчилдөггүй боловч автомат бөгөөд ихэнхдээ хэрэглэгчид харагддаггүй үйлдлийн системүүдийг ашиглан идэвхитэй санах ойн хэсэгт суудаг өөрийгөө олшруулдаг вирус юм. Тэдгээрийн хяналтгүй олшролт нь системийн нөөцийг зарцуулж бусад даалгавруудыг удаах болон зогсоодог.

Трояны морь нь хэрэгтэй ба/эсвэл аюулгүй мэт байдаг боловч үнэн хэрэгтээ нуугдсан програмууд эсвэл коммандын скриптыг зогсоож, системийг халдлагад өртөмхий болгох хортой ажиллагаатай юм.

**БҮГД НАЙРАМДАХ СОЛОНГОС УЛСЫН 1.25 ИНТЕРНЭТ ХЯМРАЛ**

2003 оны 1 сарын 25-нд 'Slammer worm' гэх компьютерийн вирус Бүгд Найрамдах Солонгос улсад орон даяар интернэтийн холболт тасалдахад хүргэсэн юм. 9 цаг гаруй үргэлжилсэн энэхүү тасалдал нь өтний улмаас устгагдсан домэйн нэрийн сервер (DNS)-ээс шалтгаалан үүссэн байна. Энэхүү тасалдалын улмаас онлайн их дэлгүүрүүдийн алдагдал 200,000– 500,000 ам.долларааp тоологдож, онлайн худалдааны алдагдал 22.5 тэрбум ам.долларт хүрсэн байна. Хохирогчид нь энгийн хэрэглэгчид байсан учраас Сламмер ворм worm вирусын учруулсан хохирол КодРед болон Нима гэх өтнүүдийн учруулсан хохирлоос илүү их байсан байна.

Тус интернэт хямрал нь Солонгосын засгийн газраас интернэтийн үйлчилгээ эрхлэгчид (ISP) болон мэдээллийн аюулгүй байдлын компаниудад зориулсан иж бүрэн менежментийг авч хэрэгжүүлэхэд нь түлхэц өгсөн байна. Мэдээллийн дэд бүтцийн хамгаалалт ба мэдээллийн аюулгүй байдлын үнэлгээний системүүд бий болсон бөгөөд байгууллага бүрт мэдээллийн аюулгүй байдлын байгууллага болон хороо байгуулагдсан байна.

### 3. Хувь хүний мэдээллийг цуглуулж халдлага хийх буюу Social engineering

"Social Engineering" гэх нэр томъёо нь нууц мэдээллийг задлахын тулд хүмүүсийг ашиглахдаа хэрэглэдэг техникийг илэрхийлдэг. Хэдийгээр энэ нь нууц задруулалт болон залилантай төстэй боловч энэхүү нэр томъёог хууль бусаар мэдээлэл цуглуулах болон компьютерийн систем рүү нэвтрэх үйл ажиллагааг тодорхойлоход ашигладаг. Ихэнх тохиолдолд халдагч нь хохирогчтой нүүр тулдаггүй. Санхүүгийн залилан үйлдэх зорилгоор хувийн мэдээллийг интернэтээр дамжуулан хулгайлах үйлдэл болох фишинг[1] нь үүний жишээ юм. Фишинг нь интернэт дэх ноцтой гэмт хэргийн үйл ажиллагаа болоод байна.

**ШВЕДИЙН БАНК "ХАМГИЙН ТОМ" ОНЛАЙН ХУЛГАЙД ӨРТСӨН ТУХАЙ**

2007 оны 1 сарын 19-нд Шведийн Норди банк онлайн фишингд өртсөн. Халдлага нь банкны нэрээр зарим үйлчлүүлэгчид рүү нь илгээсэн өөрчлөлт хийсэн Троянаар эхэлсэн байна. Илгээгч нь үйлчлүүлэгчдийг 'спамтай тэмцэх' аппликэйшнийг татаж авахыг уриалсан байна. raking.zip' болон 'raking.exe' гэсэн нэртэй хавсаргасан файлыг татаж авсан хэрэглэгчдэд зарим хамгаалалтын компаниудын 'haxdoor.ki' гэж нэрлэдэг Троян халдварласан байна. Хаксдоор нь товчлуурын даралтыг бичихийн тулд килоггерыг суулгаж рүүткит ашиглан өөрийгөө нуудаг. Трояны .ki хувилбарын пэйлоад нь хэрэглэгч Норди онлайн банкны системд холбогдох оролдлого хийхэд идэвхжсэн байна. Хэрэглэгчийг нэвтрэх дугаар гэх мэт нэвтрэх мэдээллээ оруулах хуурамч хуудас руу чиглүүлдэг. Хэрэглэгч мэдээллээ оруулсны дараа алдаа заасан санамж гарч тэдэнд сайт техникийн сааталд орсон тухай мэдээлсэн байна. Дараа нь гэмт этгээдүүд үйлчлүүлэгчдийн данснаас мөнгө авахын тулд цуглуулсан үйлчлүүлэгчийн мэдээллийг жинхэнэ Нордигийн вебсайт дээр ашигласан.

Энэхүү троян агуулсан и-мэйл Нордигийн үйлчлүүлэгчид рүү 15 сарын турш илгээгдсэн байна. Банкны хоёр зуун тавин үйлчлүүлэгч үүнд өртсөн гэж мэдээлж байгаа ба хохирол 7-8 сая Швейцарь кроны (USD 7,300–8,300) хооронд тоологдож байна. Энэ тохиолдол нь кибер халдлага өндөр төвшний аюулгүй байдлын хамгаалалттай санхүүгийн компаниудад ч нөлөөлөх чадвартай болохыг баталж байна.

*Эх сурвалж: Tom Espiner, "Swedish bank hit by 'biggest ever' online heist," ZDNet.co.uk (19 January 2007), http://news.zdnet.co.uk/security/0,1000000 189,39285547,00.htm*

## *Бусад хакерийн тактикууд*

### 4. Dumpster diving - хогийн сав ухах

[1] фишинг нь хүмүүсийг хуурах замаар өөрт хэрэгтэй мэдээлэл олж авахыг хэлээд байгаа юм. голдуу хэрэглэгчийн дансны мэдээлэл болон нэвтрэх нэр, нууц үг хулгайлах зорилгоор хийгддэг.

Компаний компьютерууд руу дайрч ороход туслах мэдээллийг хайж олохын тулд тэдний хогийн савыг нарийн шалгадаг арга юм. Үүний хамгийн гол давуу тал бол хууль ёсны байж чаддаг гэхдээ хэн ч хаясан хогоо ухуулах дургүй нийгмийн талаас хамгаалалтанд байдаг гэж ойлгож болно. Хэн нэгний хэрэггүй гээд хаяаад орхисон зүйлийг авж болно энэ нь мэдээллийн алтны уурхай ч байж болох юм. Хакерийн гол үйл хөдлөл бол хүмүүсийн харилцаа их явагддаг тэр хэсэгт оршино. Нууц үг , хэрэглэгчийн нэр гэх мэт. Dumpster diving hacker нь дараах зүйлийг хайдаг

1. Утасны жагсаалт – Энэ нь компаний бүтэц зохион байгуулалт, байж болох нэр зэрэг мэдээлийг өгнө.
2. Тэмдэглэл - Дотор болсон үйл ажиллагааг мэдэх
3. Календарчилсан тэмдэглэлт өдрүүд – Энэ нь ажилчид байхгүй ажиллахгүй байх үеийг зааж өгнө.
4. Хуучин хэрэглэхээ больсон хатуу диск – Хуучин мэдээллийг сэргээж бүх үйл хөдлөлийг мэдэж болно. (Б.Батхишиг, Д.Чинзориг, Энхбилгүүн, Пагамноржин, Мөнхшүр, 2012)

**5. War dailing - Дайралт хийн залгах**

Модемын холболтоор дамжуулан холбогдох замыг хайх зорилгоор мянган мянган телефон утасны дугаар руу автоматаар залгадаг програмууд юм. Гол зорилго нь компьютерийн ялангуяа байгууллагын дотоод сүлжээрүү нэвтрэх чадвартай утасны дугаарыг хайж олох зорилготой юм.

**6. Logic bomb – Логик бөмбөг**

Энэ нь өөрийгөө хувилан олшруулдаггүй учраас яг вирус биш юм. Тэд өөрсдийн байгаа байдлаараа програм биш юм шиг боловч үнэн хэрэгтээ өөр програмын зүсээ хувилгасан хэсэг байдаг. Түүний гол зорилго нь тохиромжтой нөхцөл бүрдэнгүүт дискэн дээрх өгөгдлийг устгах, эвдэх зэрэг үйлдэл хийдэг. Logic bomb нь ачаалагдах хүртлээ илэрдэггүй учраас үр дүн илүү хор хөнөөлтэй. Үйлдлийн систем хэрэглээний програмд нууцаар оруулсан код. Тодорхой нөхцөл бүрдэх, тогтоосон цаг хугацаа болох, гаднаас команд өгөхөд идэвхжиж сүйтгэх үйлдэл, нөлөөлөл үзүүлнэ. Зарим үйлдвэрлэгчид бүтээгдэхүүнийхээ бүрдэл хэсгүүдэд суулгаж үйлдвэрлэдэг, мэдээллийн дайны зэвсэг болгон ашигладаг. (Хулан, Туяана, Түмэннасан, 2012 он)

**7. Buffer overflow – Буффер[2] дүүргэх**

Компьютерийн санах ойны буфер руу маш их хэмжээний өгөгдөл илгээх замаар компьютерийн хяналтыг сүйтгэх эсвэл эзэмдэх арга юм. Гол ажиллагаа нь программруу өгөгдөл оруулахад ажиллаж эхлэх бөгөөд ингэснээр программын ажиллагаа болон гаралтын утгыг өөрчилдөг байна. Буффер дүүргэлтийн олон хувилбарууд байдаг бөгөөд үндсэн 2 төрөл нь stack based болон heap based юм.

**8. Sniffer - Үнэрлэгч**

Энэ нь таны нууц үгийг илгээх үед замаас нь хулгайлах арга. Энэ бол нэлээд мэргэжлийн хакерууд, эсвэл нэлээд хүчтэй хакер програм ашиглаж хийдэг. Ихэвчлэн yahoo messenger, msn messenger зэрэг өргөн хэрэглээний интернет програмуудаас нууц үгийг хулгайлдаг. Мөн маш олон

[2] Өгөгдлийн ижил нэгэн төрлийг агуулсан, үргэлжилсэн(өөрөөр хэлбэл дундаа тасраагүй), компьютерийн санах ойн хэсгийг Буффер гэнэ.

хулгайч вирусууд байдаг ба таны веб хөтөч программаа оруулсан нууц үг, кредит картны дугаарыудыг хулгайж вирусын эзэн рүү илгээдэг. Иймээс та аль болох аюулгүй үйлдлийн систем, маш сайн вирусын програмыг сонгож байх нь зөв юм. Бас нэгэн аюултай үйлдэл бол интернет кафе ашиглах. Бусад газар ямар байдгийг сайн мэдэхгүй ч Монгол дахь интернет кафенуудын хувьд ямар ч хяналт байдаггүй. Тиймээс интернет кафегаас майлээ шалгасан бол дараа нь нууц үгээ аль болох хурдан сольж байх нь дээр. Ер нь интернет кафегаас ямар нэгэн сайт руу орсон бол та нууц үгээ алдах магадлал маш өндөр гэдгийг санаарай. (http://dusal.blogmn.net, 2007)

**НУУЦ ҮГ ҮҮСГЭХ ЗӨВЛӨГӨӨ:**

Ер нь нууц үг маань богино, зөвхөн нэг үг, утасны дугаар, төрсөн өдөр г.м зүйлс оруулбал маш амархан алдаж нууц үг гэдэг утгаа алддаг. Бас компьютерын чадал өдөр ирэх тутамд нэмэгдэж байгаа тул нууц үгийг тайлах аргууд ч улам боловсронгуй хялбар болж байна. Иймээс та нууц үгээ 12-оос доошгүй том жижиг үсэг тоо болон бусад тэмдэгтүүд холилдуулж сонгож байх хэрэгтэй. Мөн өөрийн хэрэглэдэг хуудас бүртээ өөр өөр нууц үг ашиглаж байх нь илүү байдаг. Жишээлбэл:Саит бүрийн домаин нэрний аль нэг хэсгийг өөрийн нууц үгэндээ хавсрагадаг байж болох юм. Таны дуртай нууц үг: evoL247 гэж бодъё. Тэгвэл:

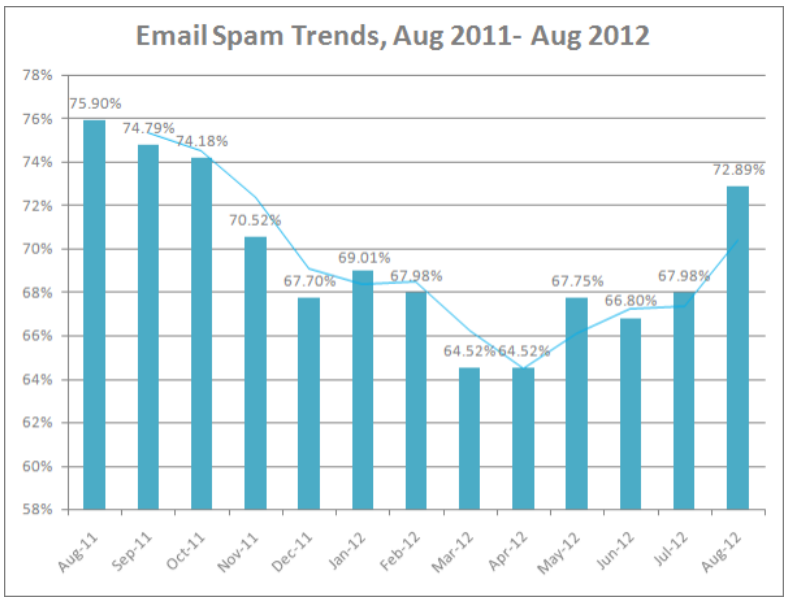
yahoo.com - aevoL247.MO+o

blogmn.net - levoL247.TE+n

google.com - oevoL247.MO+e г.м байдлаар өгөөд сурчихвал амар. Жишээ нь энд би нууц үг зохиохдоо дараах алгоритмыг баримталлаа: домайн нэрний эхнээсээ 2 дахь үсэг, миний дуртай үг, цэг, домайн нэрний өргөтгөлийн арын хоёр үсгийг араас нь аваад том үсгээр, нэмэх тэмдэг, домайн нэрний өргөтгөлийн өмнөх сүүлийн тэмдэгт. Иймэрхүү байдлаар саит болгон дээр өөр нууц үгийг өгөх хэрэгтэй. Дээрх бол зөвхөн жишээ бөгөөд та өөрийнхөө алгоритмыг

### *Дэд бүтцийн халдлагын нэмэгдэж буй аюул*

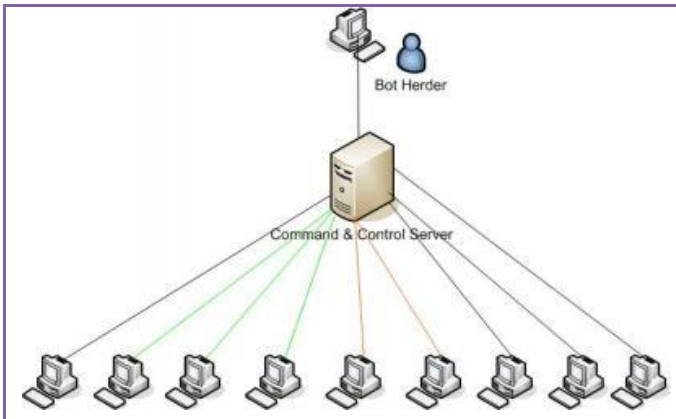
Дэд бүтцийн халдлага нь интернэтийн гол бүрэлдэхүүн хэсгүүдэд нөлөөлөх халдлагууд юм. Интернэт дэх олон тооны байгууллагууд болон хувь хүмүүс, тэдний өдөр тутмын ажил интернэтээс ихээхэн хамааралтай байдаг зэрэг нь эдгээрийг тулгамдсан асуудал болгож байгаа юм. **Ботнет** бол дэд бүтцийн халдлагын нэг жишээ юм. “ботнет-botnet” гэдэг нэр томъёо нь “командын хяналтын сервер[3]”-ээр алсын зайнаас удирдагддаг халдвартай компьютерүүдийн бүлгийг хэлдэг. Халдвартай компьютерүүд нийт сүлжээний системд өт, вирусыг тараадаг.




Ботнетийн хэрэглээний улмаас спам хурдацтай өсч байна. **Спам** нь албан ёсоор илгээгдээгүй и-мэйл, мессенжер, хайлтын хэрэгсэл, блогууд тэр бүү хэл гар утсаар дамжих боломжтой нийтийг хамарсан мессежүүд юм.

**Зураг 0-2. Спамын нийт мэйлд эзлэх хувь. Эх сурвалж: http://www.emailtray.com**

## *Ботнет/Botnet/ гэж юу вэ?*

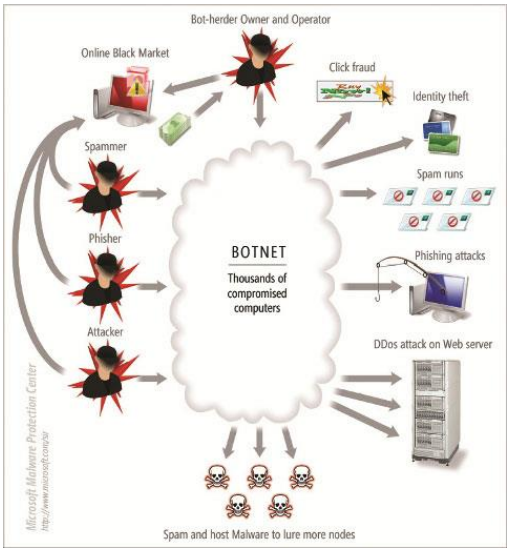



*Ботнет гэдэг нь хэдэн арваас авахуулаад хэдэн сая тооцоолуурыг гартаа оруулсан этгээдийн интернетийн сүлжээ юм. Bot өгөгдсөн тушаалыг үг дуугүй гүйцэтгэхэд бэлэн болсон тооцоолуур, Net интернет гэж ойлгож болно.*

***<u>Ботнетийн үндсэн ажиллагаа нь хэрхэн явагддаг вэ?</u>***

*Ботнет нь үдсэн хоёр хэсгээс тогтдог. Үүнд 1. C&C/Command and Control/ буюу үндсэн удирдах хэсэг. 2. Ботууд.*

- *Бот болсон тооцоолуур C&C-тэй холбогдож тушаал хүлээнэ.*
- *C&C-гээс нийт эсвэл заасан нэг бот-д тушаал өгнө.*




- *Харин ботууд өгөгдсөн тушаалыг гүйцэтгээд үр дүнг заасан замаар эзэндээ мэдээлэх болно.*
- *Мөн бот бүр нь цааш тархах оролдлого байнга хийж байдаг юм.*

***<u>Сүүлийн үеийн ботнетууд юу хийдэг юм?</u>***

- *DDoS - Сервер доголдуулах, үйлчилгээ зогсоох /тухайн системийн хүчин чадлаас давсан өгөгдөл илгээн ачаалалд оруулж систем дээр доголдол гаргах./*
- *Spam - Спам илгээх*
- *Fraud click - Хуурамч даралт өгөх*
- *Phishing - Фишинг хийх*
- *Identity theft - Хувийн мэдээллийг хулгайлах*
- *Malware - Элдэв хортой програм тараах*

***<u>Ботнетийн үнэ ханш хэд гэдэг юм бол?</u>*** *Kaspersky-гийн нэгэн нийтлэлд*

- *DDoS халдлага $50 - хэдэн мянган $ хүрдэг ба энэ хэдэн цаг үргэлжлэхээс хамаарна.*
- *Банкны данс хулгайлах $1-$1500 орчим ба тухайн дансны балансаас хамаарна.*
- *Хувийн мэдээлэл хулгайлах US-гийн иргэний мэдээлэл бол $5-$8 харин EU-гийн иргэн бол үнэ нь 2-3 дахин өсдөг байна.*
- *имайл жагсаалт нэг сая хаяг $20-$100*
- *Хортой програм тараах 30cent-ээс $1.50/суулгалт бүр дээр.*

## ХАЛДЛАГЫН ЗОРИЛГЫН ӨӨРЧЛӨЛТ

Компьютер болон сүлжээний халдлагыг сониуч зангийн улмаас эсвэл хувь хүн зугаацах зорилгоор үйлддэг гэж ойлгодог байлаа. Одоо ихэвчлэн мөнгө, нэр төр гутаах болон хорлон сүйтгэх зорилготой болсон. Түүнчлэн эдгээр төрлийн халдлагууд нь кибер гэмт хэргийн өргөн хүрээний жижигхэн хэсгийг л төлөөлдөг. **Кибер гэмт хэрэг** гэдэг нь улс төр, эдийн засаг, шашин эсвэл үзэл суртлын шалтгаанаар дижитал мэдээлэл эсвэл мэдээллийн урсгалыг зориудаар сүйтгэн тасалдуулах ажиллагаа юм. Хамгийн түгээмэл гэмт хэрэгт хууль бус нэвтрэлт, ҮБ, хортой код болон Social engineering орно. Сүүлийн үед кибер гэмт хэрэг нь үндэсний аюулгүй байдалд үзүүлэх сөрөг нөлөөгөөрөө кибер халдлага ба кибер дайны нэг хэсэг нь болоод байна.

| Орлого | Тухайн-ханш (Ам.доллараар) |
|---|---|
| Давтагдашгүй аюултай програм (adware) суулгалт бүрт төлөх төлбөр | АНУ-д 30 цент, Канадад 20 цент, Англид 10 цент, бусад газарт 2 цент |
| Аюултай програмын багц (Malware package), үндсэн хувилбар | $1,000 - $2,000 |
| add-on үйлчилгээ бүхий аюултай програмын багц | $ 20-с эхлээд ханш нь өөр өөр |
| Ашиглах багцын түрээс – 1 цаг | $ 0.99 - $ 1 |
| Ашиглах багцын түрээс – 2.5 цаг | $ 1.60 - $ 2 |
| Ашиглах багцын түрээс – 5 цаг | $4, өөр байж болно |
| Мэдээлэл хулгайлах тодорхой нэг Трояны илрээгүй хуулбар | $80, өөр байж болно |
| Тархсан үйлчилгээг бусниулах довтолгоо (ҮБ) | Өдөрт $100 |
| 10,000 халдлагад өртсөн PC | $1,000 |
| Хулгайлагдсан банкны дансны эрх | $50-с эхлээд ханш нь өөр өөр |
| 1 сая цэвэр цуглуулсан (freshly-harvested) и-мэйл (гэрчлэгдээгүй) | Чанараас хамаарч $8 хүртэл |

**Зураг 0-3. 2007 онд кибер гэмт хэргээс олсон орлого. Эх сурвалж:Trend Micro, 2007 Threat Report and Forecast (2007), 41,http://trendmicro.mediaroom.com/file.php/66/2007+Trend+Micro+Report_FINAL.pdf**

### *Халдлага эсэргүүцэх технологи*

Халдлага эсэргүүцэх технологиуд нь хадгалалт ба системийн төвшний халдлага, аюулаас хамгаалдаг. Энд дараах технологиуд орно. Үүнд:

Криптограф (Cryptography) – нууцлал гэж нэрлэгддэг криптограф нь мэдээллийн өөрийн эх хэлбэрээс (ил бичвэр /plaintext/ гэж нэрлэдэг) кодчилсон, ойлгомжгүй хэлбэр (ciphertext гэж нэрлэдэг) лүү буулгах явц юм. Код тайлалт (decryption) нь кодчилсон текстийг авч буцаан үндсэн хэлбэр лүү нь оруулах явцыг хэлдэг. Криптографыг төрөл бүрийн аппликэйшнийг хамгаалахад ашигладаг.

Нэг-удаагийн нууц үг-ННҮ (One-Time Passport-OTP) – нэрнээс нь харахад, нэг удаагийн нууц үгийг зөвхөн нэг удаа ашиглаж болно гэсэн үг. Тогтмол нууц үгүүд нь алдагдах болон хулгайд өртөхдөө амархан байдаг. Энэ эрсдлийг ННҮ-ээр хийдэг шиг нууц үгээ тогтмол

өөрчлөх замаар бууруулах боломжтой. Энэхүү шалтгааны улмаас ННУ-ийг онлайн банкны үйлчилгээ зэрэг цахим санхүүгийн гүйлгээг хамгаалахад ашигладаг.

Галт хана (Firewall) –энэ нь өөр өөр итгэмжлэлийн төвшинтэй компьютерийн сүлжээнүүд хооронд, тухайлбал ямар нэг итгэмжлэлийн бүсгүй интернэт ба хамгийн өндөр төвшний итгэмжлэл бүхий дотоод сүлжээ хоорондын зарим хөдөлгөөний урсгалыг зохицуулдаг.

Эмзэг байдлыг шинжлэх хэрэгсэл –халдлагын аргуудын тооны өсөлт болон түгээмэл хэрэглэгддэг програмуудад байх эмзэг талуудаас шалтгаалан системийн эмзэг байдлыг тодорхой цаг хугацаанд үнэлж байх шаардлагатай. Компьютерийн аюулгүй байдлын хувьд эмзэг байдал бол халдлага үйлдэгчид систем рүү нэвтрэх боломж олгодог сул тал нь юм.Сүлжээнй эмзэг байдлыг шинжлэх хэрэгсэл нь рутер, галт хана сервер зэрэг сүлжээний нөөцийн эмзэг байдлыг шнжилдэг. Серверийн эмзэг байдлыг шинжлэх хэрэгсэл нь дотоод систем дэх сул нууц үг, сул тохиргоо болон файлын зөвшөөрлийн алдааг эмзэг байдал гэж үзэн шинжилдэг. Энэхүү хэрэгсэл нь дотоод систем дэх илүү олон эмзэг байдлыг шинжилдэг учраас серверийн эмзэг байдлыг шинжлэх хэрэгсэл нь сүлжээнй эмзэг байдлыг шинжлэх хэрэгсэлтэй харьцуулахад харьцангуй бодит үр дүн өгдөг.

### *Халдлага илрүүлэх технологи*

Илрүүлэх технологийг сүлжээ ба чухал системүүд дэх хэвийн бус байдал болон сэжигтэй нэвтрэлтийг илрүүлэн арилгахад ашигладаг. Илрүүлэлтийн технологид дараах орно:

1. Антивирус –Антивирус програм хангамж бол өт, фишинг халдлагууд, рүүткит, трояны морь болон бусад малвэйр гэх мэт хортой кодыг илрүүлж, арилгах зориулалт бүхий компьютерийн програм юм.

2. Довтолгоон илрүүлэх систем-ДИС (Intrusion Detection System -IDS) – ДИС нь болзошгүй аюулгүй байдлын зөрчлийг илрүүлэхийн тулд компьютер, эсвэл сүлжээн доторх төрөл бүрийн талбараас мэдээлэл цуглуулан шинжилдэг. Халдлага илрүүлэх функцүүдэд хэвийн бус ажиллагааны дүн шинжилгээ ба халдлагын хэлбэрийг таних чадвар зэрэг орно.

3. Довтолгооноос сэргийлэх систем-ДСС (Intrusion prevention system -IPS) – Довтолгооноос сэргийлэх систем нь болзошгүй аюулыг олж илрүүлэн, тэдгээрийг халдлагад ашиглахаас нь өмнө хариу арга хэмжээ авахыг хичээдэг. ДСС нь сүлжээний хөдөлгөөнийг хянаж учирч болох аюулын эсрэг сүлжээний администраторын тогтоосон журмын дагуу шуурхай арга хэмжээ авдаг. Жишээлбэл, ДСС сэжиг бүхий IP хаягнаас ирэх хөдөлгөөнийг хааж болно.

### *Хувийн эрх чөлөөний асуудлууд*

**Хувийн эрх чөлөө, амгалан байдлыг зөрчих** - Хүмүүсийн хувийн имэйлийн харилцаа болон компьютерт хадгаласан зүйлүүдэд хандах, Хувь хүмүүсийн орсон Интернетийн вэб сайтуудааас тэдний тухай мэдээлллийг цуглуулах, дундаа ашиглах зэрэг нь тухайн хүний талаар мэдээллийг зөвшөөрөлгүй цуглуулах эргээд тэдгээр мэдээллийг ашиглан төрөл бүрээр хэрэглэгчийг хохироох явдлууд гарч байна

**Компьютерийн хяналт** - Тухайн хүнийг хаана байгааг байнга мэдэж байх, ялангуяа гар утас ба пейжерийн үйлчилгээнүүд газар байршлаас илүү хүмүүстэй илүү ойр ажиллаж байна.

**Компьютераар тааруулах**- Бизнесийн өөр бусад үйлчилгээнүүдийг сурталчлахын тулд олон эх сурвалжаас олж авсан хэрэглэгчийн мэдээллийг ашиглан түүнийг хайх, мэдээллийг нь тааруулах

**Хувь хүний зөвшөөрөлгүй файлууд** - Хувь хэрэглэгчийн дүр төрхүүдийг гаргахын тулд утасны дугаар, зээлийн картын дугаар, имэйл хаяг болон бусад хувийн мэдээллийг цуглуулах зэрэг нь тухайн хүний зөвшөөрөлгүйгээр хувийн мэдээлэл эрх чөлөөнд нь халдаж байгаа хэрэг юм. Байгууллагуудын

хувьд эдгээр мэдээллийг хууль бусаар ашиглахгүй гэж байгаа боловч эхлээд мэдээллийг олж авч байгаа арга нь буруу хийгээд цаашид тэрхүү мэдээллийг найдвартай хамгаална гэсэн баталгаа байхгүй байдаг

*Бусад сорилтууд*

- **Ажил эрхлэлт** - МТ нь шинэ шинэ ажлуудыг бий болгож, бүтэмжийг дээшлүүлж байна. Гэвч бас ажлын боломжуудыг, мөн шинэ ажлуудад шаардлагатай янз бүрийн ур чадваруудыг үлэмж хэмжээгээр бууруулах шалтгаан болж чадна.
- **Компьютерийн хяналт** - Ажиллагсдын ажиллаж байгаа төлөв, бүтээмжийг хянахад компьютеруудыг хэрэглэж болно
- **Ажиллах нөхцөл** - МТ нь IT нэг янзын эсвэл дургүй хүрмээр ажлуудыг халж байна. Гэвч ур чадвартай гар урлаач, дарханыг шаарддаг зарим ажлууд өдөр тутмын, давтагддаг ажлууд эсвэл байнгын бэлэн байдаг үүрэг хүлээдэг ажлуудаар солигдож байна.
- **Хувь хүний онцлог** - Компьютерууд хүмүүсийн хоорондын харилцаа, хамаарлыг үгүй болгож байгаа учраас үйл ажиллагаанд байдаг хүнлэг чанарыг алдагдуулж, хувь хүний чанарыг алдагдуулж байна. Жишээ нь: Уян хатан бус системүүд

***Эрүүл мэндийн асуудлууд***

**Carpal Tunnel Syndrome** - Гар ба бугуйны зовиуртай гэмтлийн өвчин бөгөөд маш өргөн тархаад байгаа өвчний нэг юм. Хамгийн гол сэргийлэх арга нь тодорхой хугацаанд гар бугуйны дасгалыг тогтмол хийж занших хэрэгтэй юм.

**Нурууны өвчин:** Олон ажилчид нэгэн асуудалтай байнга тулгардаг нь нурууны өвчин юм. Компьютерийн өмнө тухгүй, эвгүй сууснаас, эсвэл хямд төсөр, чанар муутай сандал дээр сууснаас болоод нурууны ноцтой эмгэг үүсэх эхлэл тавигддаг.

Сэргийлэх арга:

Бүрэн дүүрэн тохиргоо хийх боломжтой сандал дээр суух.

Хөлөө байнга тавиур дээр тавих нь нурууны эмгэгээс урьдчилан сэргийлнэ.

Мөн дэлгэцээ бага зэргийн налуу байлга. Тэгвэл эвгүй хэцүү хөдөлгөөн, нуруугаараа эвгүй эргэх, тонгойх зэргээс зайлсхийх болно.

**Хуруу, гарын эмгэг**: Урт хугацааны турш нэг хөдөлгөөнөө дахин давтан хийсээр гэмтэлд учрах магадлалтай эрхтэнд хуруу гар, бугуй зайлшгүй тооцогддог.

– Сэргийлэх арга:

- Гол нь байрлал тун зөв байх ёстой. Хэрвээ тасралтгүй юм бичиж байгаа бол нэг цаг тутамд ойролцоогоор 5 минутын хугацаатай хуруу гараа амарааж байх хэрэгтэй.

**Нүдний хараа:** Компьютерийн дэлгэцийг удаанаар ширтвэл нүд эцэх нь ойлгомжтой. Ялангуяа гэрэлтүүлэг бүүдгэр муу, эсвэл хэт хурц гэрэлтэй, дээр нь дэлгэц жаахан л чичирхийлэлтэй бол нүдний харааг шууд муутгадаг гэдгийг дээр хэлсэн.

– Сэргийлэх арга:

- Дэлгэцийн хортой туяаг бууруулдаг дэлгэц хамгаалагч хэрэглэж, дэлгэц өчүүхэн төдий гэмтэж ямар нэгэн согогтой болсон л бол цаашид хэрэглэх хэрэггүй.
- Тасралтгүйгээр нэг цагаас илүү ажиллаж болохгүй гэсэн энгийн дүрмийг зайлшгүй мөрд.
- Дэлгэцийн өнгийг өрөөний гэрэлтэй нийцүүлэн тохируулах ёстой. Монитрын доор хэсэгт байрласан тохиргооны товчлууруудаар энэ тохиргоог хийнэ.
- Хурц гэрэлтэй үед цонхны хөшгөө татаж гэрэлтүүлгийн асуудлаа шийдэж болно.

**Хэт ягаан туяа цочрол**: Лазер принтер болон хувилагч машинаас ялгардаг хэт ягаан туяа ажилчдын амьсгалын асуудалд муугаар нөлөөлдгийг эмч нар байнга сануулдаг.

- Сэргийлэх арга:
  - Ажилчдын сууж байгаагаас дор хаяж нэг метрийн зайд принтерээ байрлуулах нь хамгийн зөв арга болох ба талбайн агааржуулалтад тэр бүр нөлөөлөхгүй.
  - Хувилагч машинаа аль болох ажилчдаас зайтай, коридорт юм уу эсвэл өрөөний үүд хавьцаа байрлуулж болно. (http://phi.moh.gov.mn/, n.d.)

### *Эргономик буюу ажлын орчин*

- **Өрөөний температур, агааржуулалт, чийг**

Өрөөний ямар ч нөхцөлд зохицон тэсэх чанар ажилчид бүрт өөр өөр. Гэсэн ч ажлын бүтээмж, болон ажилчдын хувцаслалт, эрүүл мэнд зэрэгт өрөөний температур заавал нөлөөлдөг. Өөрөөр хэлбэл өрөөний температур нь оффисын орчны ая тухтай байдал болоод ажилчдын эрүүл мэндийг голлог шийднэ гэсэн үг. Оффисын өрөөний температур хамгийн багадаа 16 хэм байх ёстой. Хэт хүйтэн эсвэл хэт халуун бол ажилчдын биед сөргөөр нөлөөлөх нь дамжиггүй. Гэхдээ өрөөний температурт бас өөр олон зүйлүүд нөлөөлдөг. Үүнийг тун сайн бодолцох хэрэгтэй. Жишээ нь: оффисын чинь цонх урагшаа харсан уу үгүй юу, эсвэл гадна хаалга тань ямар вэ, ямар хэмжээтэй өрөөнд хэдэн хүн суудаг вэ гэх зэрэг олон зүйлүүд нөлөөлнө. Өрөөний цонх урагшаа харсан бол нарны энерги тусч арай илүү дулаан болно, гадна хаалга өөрөө хаагддаг механизмтай бол гаднаас хүйтэн орохгүй, жижигхэн өрөөнд олон хүн суудаг бол энэ өрөө арай илүү халуун болж, агааржуулалт илүү хэрэгтэй гэх зэргээр олон олон зүйлүүд байна. Бас өрөөнд компьютер их байвал өрөөний халуун бага хэмжээгээр нэмэгдэхээс гадна агаарын хуурайшилт үүсэх нь их байна. Зөвлөгөө: Өрөөний температур, агаарын урсгал, чийглэг нь компьютерт нөлөөлөх том хүчин зүйлүүдийн нэг юм.

- **Чимээ, шуугиан**

Нэг том талбайд ажилладаг оффисын ажилчид бие биеэсээ хамааралтай байх нь ойлгомжтой. Тэд бие биенийхээ анхаарлыг сарниулж, ажлын үр дүнг бууруулах магадлал өндөр байдаг. Гэхдээ эмх цэгцтэй, сахилга баттай ажлын байранд чимээ шуугианы асуудал огтхон ч том зүйл биш. Энэ нь хувь хүний ухамсраас шалтгаалах зүйл юм. Нөгөө талаар ажилчид өөрсдөө дэг журамтай байлаа ч компьютер болон бусад төхөөрөмжүүдийн гаргадаг чимээ шуугианыг яалтай билээ. Тухайлбал принтер, хувилагч машин болон компьютер ч гэсэн ихээхэн дуу чимээ гаргаж, ажилчдыг ихээр ядрааж, улмаар толгой өвдөхөд хүргэдэг.Зөвлөгөө: Принтер, хувилагч машин гэх мэт чимээ шуугиантай төхөөрөмжүүдээ ажилчдын байгаа байрлалаас арай зайдуу тавьж болно. Эсвэл өөр дээр нь байрлах дуу намсгагчаар /Зарим төхөөрөмжүүд дуу намсгагчтай байдаг/ дууг нь багасгаж болно. Өөр нэг зөвлөгөө гэвэл оффисын байрандаа засвар хийж дуу авиа шингээгч суурилуулах боломж бий ч өндөр зардалтай.

- **Гэрэлтүүлэг**

Оффисын гэрэлтүүлэг нь харааны бэрхшээл үүсгэхгүй байх ёстой. Өөрөөр хэлбэл хэт бүүдгэр биш, хэт хурц биш, кейбордын үсэг болон дэлгэц дээрх мэдээлэл ямар ч бэрхшээлгүй уншигддаг байх ёстойг анхаарах шаардлагатай. Энд ширээний гэрэл ч ашиглаж болно, гол нь тохиромжтой байх хэрэгтэй. Хэрэв оффисын гэрэл хэт хурц тод бол толгой өвдөж, нүд бүрэлзэж болзошгүй. Тэгэхээр цонхныхоо хөшгөөр зохицуулж болно. Харин бүүдгэр бол цонхоороо байгалийн гэрэл оруулах хэрэгтэй. Байгалийн гэрэл мэдээж хор нөлөө багатай.

1. Тохиромжтой гэрэлтүүлэг
2. Ширээний гэрэл – хэт хурц биш, гялбахгүй



3. Анхаарал сарниулах дуу чимээ бүхий төхөөрөмж. Гэхдээ дууг нь хамгийн бага болгож намсгасан.
4. Хөлийн хэсэг - чөлөөтэй хөдөлж чадах хангалттай зайтай
5. Цонхны хөшиг
6. Зохистой програм хангамж буюу дэлгэц дээрх мэдээлэл шууд уншигдана
7. Дэлгэц – тогтвортой дүрстэй, мэдээлэл шууд уншигдана, гэрэл ойхгүй, тохиргоо хийх бүрэн боломжтой дэлгэц
8. Кейборд – ашиглахад хялбар, тохиромжтой, үсэг нь тодорхой гаргацтай
9. Ажлын ширээ – зохион байгуулалттай, эмх цэгцтэй, зай талбай сайтай, гэрэлтүүлэг сайтай ч хурц биш
10. Сандал - өөртөө нийцүүлэн тохируулж болдог сандал
11. Хөлийн тавиур (http://phi.moh.gov.mn/, n.d.)

## Эх сурвалж

*http://dusal.blogmn.net*. (2007, 12 2). Retrieved 12 9, 2012, from http://dusal.blogmn.net/9864/nuuts-ug-ayuulgui-baidal.html#2007-12-2

Б.Батхишиг, Д.Чинзориг, Энхбилгүүн, Пагамноржин, Мөнхшүр. (2012). *Семинар 11 тайлан.*

Д.Баярмаа. (n.d.). *Маркетинг.*

Хулан, Туяана, Түмэннасан. (2012 он). *Семинар11.*

хүрээлэн, Н. э. (n.d.). *http://phi.moh.gov.mn/*. Retrieved 12 10, 2012, from http://phi.moh.gov.mn/index.php?sel=suggestionmore&more=1