ОНЦ ЧУХАЛ ДЭД БҮТЦИЙГ КИБЕР ТЕРРОРИСТ ХАЛДЛАГААС ХАМГААЛАХ ТОГТОЛЦООГ БОЛОВСРОНГУЙ БОЛГОХ НЬ (БАНКНЫ САЛБАРЫН ХҮРЭЭНД)

Удирдсан багш: Б. Энх-Амгалан / Ph.D дэд профессор/

МУИС-ийн Бизнесийн сургуулийн санхүүгийн тэнхим

Илтгэгч:
Т.Биндэръяа
Б.Амарбаясгалан

АГУУЛГА

МОНГОЛ УЛСЫН ХӨГЖЛИЙН БАРИМТ БИЧИГ

Монгол Улсын үндэсний аюулгүй байдлын үзэл баримтлал

3.6.1.11-д “Кибер орчин дахь гэмт явдалтай тэмцэх, аливаа гэмт хэргийг илрүүлэх, нотлоход тооцоолох хэрэгслийн криминалистик техникийн шинжилгээ ашиглах үндэсний чадавхыг бий болгоно”

Алсын хараа - 2050

4.3 Эдийн засгийг тэтгэсэн, уян хатан, цахим технологид суурилсан олон талт санхүүгийн үйлчилгээг хөгжүүлэх, дэлхийн хөрөнгийн зах зээлд оролцох түвшний цахим санхүүгийн тогтолцоог хөгжүүлэх;

3.6.1.1-т “Мэдээллийн аюулгүй байдлыг хангах, мэдээллийн орчинд сөргөлдөх аюулаас сэргийлэх, кибер орчин дахь гэмт явдалтай тэмцэх чиглэлд олон улсын хамтын ажиллагааг өргөжүүлэн хөгжүүлнэ”

КИБЕР ГЭМТ ХЭРЭГ НЬ БАНК, САНХҮҮГИЙН САЛБАРЫН ШИНЭ СОРИЛТ БОЛОХ НЬ

Санхүүгийн үйлчилгээнд халдсан ransomware халдлага 2022 онд 55% байсан бол 2023 онд 64% болж өссөн нь 2021 онд бүртгэгдсэн 34% -иас бараг хоёр дахин их байна. Монгол Улсад 2023 онд цахим мэдээллийн аюулгүй байдлын эсрэг гэмт хэрэг 129 (49.8%)-иар өссөн байна. Үүнтэй холбоотойгоор виртуал хөрөнгийг хамгаалах, мэдээллийн нууцлалыг хангах, аливаа эрсдэлийг бууруулах, цахим гүйлгээнд итгэх итгэлийг хадгалах сорилтууд зүй ёсоор тулгаран гарч ирж байна.

АНУ

Аргентин

Бразил

БНХАУ

Монгол Улс нь НҮБ-ын дэргэдэх мэдээлэл, харилцаа холбооны технологийн асуудал хариуцсан тусгай агентлаг болох Олон улсын харилцаа холбооны нэгдэл (ITU)-ээс 2020 онд гаргасан кибер аюулгүй байдлын индексээрээ 120-т, Үндэсний кибер аюулгүй байдлын индексээрээ 137-д, Дэлхийн Мэдээлэл, харилцаа холбооны хөгжлийн индексээрээ 91-т эрэмбэлэгдсэн байна.

СУДАЛГААНЫ АРГА ЗҮЙ, ТААМАГЛАЛ

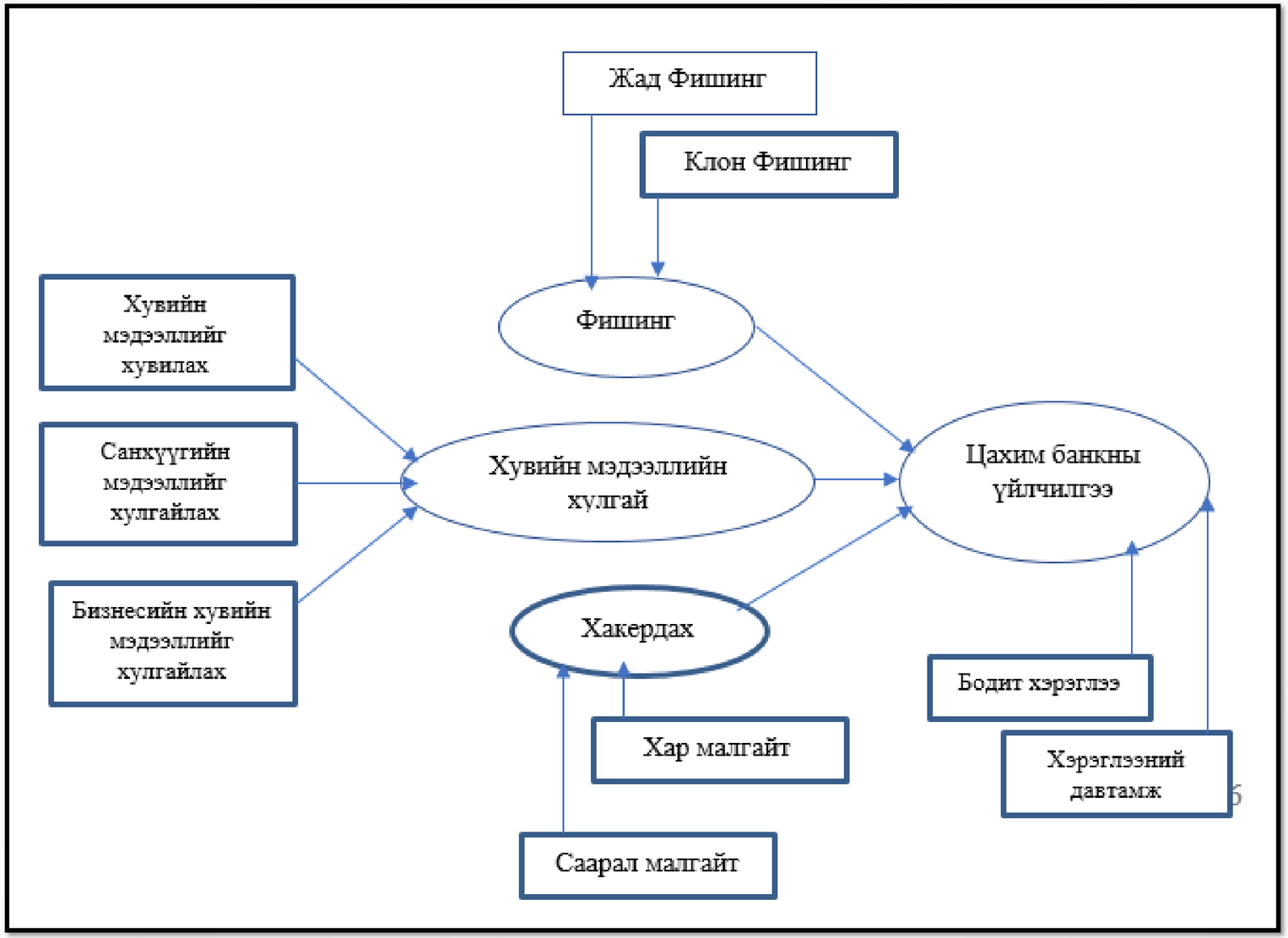
Анхдагч өгөгдлийг цуглуулахад анкетын асуулгын аргыг, хувьсагч хоорондын хамаарлын хэлбэрийг тогтоох буюу тэдгээрийн холбоо хамаарлыг илрүүлэх, энэхүү хамаарлыг үнэлэхэд регрессийн шинжилгээний аргыг ашигласан болно.

Таамаглал 1. H1: Фишинг нь цахим банкны үйлчилгээнд сөргөөр нөлөөлнө

Таамаглал 2. H2: Хувийн мэдээллийг хулгайлах нь цахим банкны үйлчилгээнд сөргөөр нөлөөлнө.

Таамаглал 3. H3: Хакердах нь цахим банкны үйлчилгээнд сөргөөр нөлөөлнө.

Санхүүгийн мэдээллийг хулгайлах – Бараа, үйлчилгээ авахын тулд бусдын хувийн мэдээллийг ашиглах;
Хувийн мэдээллийг хувилах – Өдөр тутмын амьдралдаа бусдын нэр, хаягийг ашиглах;
Бизнесийн хувийн мэдээллийг хулгайлах – Зээл авахын тулд бусдын бизнесийн нэрийг ашиглах;
Гэмт хэрэг үйлдсэн этгээдийн хувийн мэдээллийг хулгайлах – гэмт хэрэг үйлдэх бэлтгэлийг хангах өөр хүний дүр эсгэх.



Эх сурвалж: (Судлаачийн нэгтгэл, 2024)

Түүвэрлэлтийн арга

Хүснэгт 1. Хүн ам зүйн үзүүлэлт

Table N %		
Судалгаанд оролцогчдын хүйс	Эр	**56.0%**
	Эм	**44.0%**
Судалгаанд оролцогчдын гэр бүлийн байдал	Гэрлээгүй	**53.1%**
	Гэрлэсэн	**47.9%**
Судалгаанд оролцогчдын нас	18-25 нас	**30.8%**
	25-35 нас	**53.4%**
	35-50 нас	**15.8%**
	50-аас дээш нас	**0.0%**
Санал асуулгад оролцогчдын боловсролын зэрэг	Бакалавр	**30.2%**
	Магистр	**49.9%**
	Доктор	**5.5%**
	Бусад	**14.4%**

Судалгаанд оролцогчдын 56 хувь нь эрэгтэй, 44 хувь нь эмэгтэй; 53.1 хувь нь ганц бие, 47.9 хувь нь гэр бүлтэй гэж хариулсан нь судалгаанд оролцогчдын дийлэнх нь гэрлээгүй байгааг харуулж байна. Бусад ангиллыг хүснэгтэд үзүүлэв.

Хүснэгт 3. Case Processing Summary

		N	%
Cases	Valid	100	99.1
	Excluded	1	0.9
	Total	106	100.0

a. Listwise deletion based on all variables in the procedure.

Хүснэгт 4-өөс үзвэл, Cronbach's Alpha 0.71 байгаа нь өгөгдлийн найдвартай байдлыг илтгэж байна. Cronbach's Alpha утгыг ашиглан өгөгдөлд регресс болон корреляцийн шинжилгээг хийх боломжтой.

Хүснэгт 4. Онч бөгөөд найдвартай байдлын статистик

Cronbach's Alpha	N of Items
0.710	21

Корреляцийн шинжилгээ

	Phishing	Identity Theft	Hacking	E-banking Usage
Phishing	1.00	0.45	0.30	-0.25
Identity Theft	0.45	1.00	0.55	-0.35
Hacking	0.30	0.55	1.00	-0.20
E-banking Usage	-0.25	-0.35	-0.20	1.00

Цахим гэмт хэргийн төрлүүд (Фишинг, хувийн мэдээллийг хулгайлах, хакердах) болон цахим банкны ашиглалтын хоорондын сөрөг хамаарал нь ($r = -0.2$, $r = -0.25$, $r = -0.35$, $p < 0.001$) цахим гэмт хэрэгт өртсөн гэж мэдээлсэн хүмүүс цахим банкны үйлчилгээг ашиглах магадлал бага байгааг харуулж байна.

Регрессийн шинжилгээ

Predictor	Coefficient (β)	Standard Error	t-value	p-value
Intercept	3.90	0.20	19.50	<0.001
Phishing	-0.40	0.15	-2.67	0.009
Identity Theft	-0.35	0.12	-2.92	0.005
Hacking	-0.20	0.10	-2.00	0.048

$$E-bankingUsage=\beta 0+\beta 1(Phishing)+\beta 2(IdentityTheft)+\beta 3(Hacking)+\varepsilon$$

Intercept (β_0): Бүх бие даасан хувьсагч (фишинг, хувийн мэдээллийг хулгайлах, хакердах) тэг байх үед урьдчилан тооцоолсон цахим банкны хэрэглээг илэрхийлнэ.

Коэффициент (β_1, β_2, β_3, β_4): Эдгээр нь бие даасан хувьсагч бүрийн нэг нэгжийн өөрчлөлтийн хувьд хамааралтай хувьсагчийн өөрчлөлтийг (цахим банкны хэрэглээ) илэрхийлж, бусад хувьсагчдыг тогтмол байлгадаг.

СУДАЛГААНЫ ДҮГНЭЛТ

Таамаглал 1 (H1): Фишинг нь цахим банкны хэрэглээнд сөргөөр нөлөөлнө.
Регрессийн шинжилгээгээр фишингийн хувьд статистик ач холбогдолтой, сөрөг коэффициент (β = -0.40, p = 0.009) илэрсэн.

Таамаглал 2 (H2): Хувийн мэдээллийг хулгайлах нь цахим банкны хэрэглээнд сөргөөр нөлөөлнө.
Регрессийн шинжилгээгээр хувийн мэдээллийг хулгайлах гэмт хэргийн хувьд статистик ач холбогдолтой, сөрөг коэффициент (β = -0.35, p = 0.005) илэрсэн.

Таамаглал 3 (H3): Хакердах нь цахим банкны хэрэглээнд сөргөөр нөлөөлнө.
Хакердах ажиллагааны коэффициент нь статистик ач холбогдолтой (β = -0.20, p = 0.048) байсан ч энэ нь фишинг болон хувийн мэдээллийг хулгайлахтай харьцуулахад бага юм.

1. Олон шатлалт хамгаалалт: Банкууд сүлжээндээ гадны хандалтаас сэргийлж, зөвшөөрөлгүй үйл ажиллагаа, программыг блоклох найдвартай Firewalls механизмыг хөгжүүлэх шаардлагатай.

2. Ажилтнуудын сургалт: Банкны салбарын цахим гэмт хэргийн эрсдэлийг бууруулахад ажилтнуудын сургалт, сурталчилгаа чухал үүрэг гүйцэтгэдэг. Кибер аюулын шинж чанар байнга хувьсан өөрчлөгдөж байгаа тул банкны байгууллагууд ажилтнуудаа аливаа боломжит кибер халдлагыг илрүүлэх, урьдчилан сэргийлэхэд шаардлагатай мэдлэг, ур чадварыг эзэмшүүлэх нь чухал юм.

3. Кибер аюулыг цаг алдалгүй илрүүлж, хариу арга хэмжээ авахын тулд сүлжээний траффик болон гажуудсан үйл ажиллагааг идэвхтэй хянах боломжтой, санхүүгийн байгууллагуудын хооронд кибер аюулын мэдээллийг бодит цаг хугацаанд хуваалцах платформыг бий болгох нь зохистой юм.

4. Хамтран ажиллах, мэдээлэл солилцох

ЭХ СУРВАЛЖ

- Ц.Хүрэл-Очир, Кибер гэмт хэрэг: Хандлага ба төрөл, хэлбэр, Эрх зүй, сэтгэлгээ: үзэл бодол, эргэцүүлэл сэтгүүл,Уб.,2015
- Нээлттэй нийгэм форум, кибер гэмт хэргийн зохицуулалтын талаарх харьцуулсан судалгаа (Виртуал хөрөнгийн үйлчилгээ үзүүлэгчийн үүрэг, үйл ажиллагааны эрсдэлийн хүрээнд), Уб.,2022
- Anderson, K. B., Durbin, E., & Salinger, M. A. (2008). Identity theft. Journal of Economic Perspectives, 22(2), 171-192.
- A. G. Johansen, „Norton,” NortonLifeLock Available: https://us.norton.com/internetsecurity-malware-ransomware5-dos-and-donts.html .
- Khan, A. A. (2013). Preventing phishing attacks using one time password and user machine identification. International Journal of Computer Applications, 68(3), 7-11.
- Oliver Wyman and DTCC project team, „Oliver Wyman, DTCC,” 03 2018. [Online]. Available: https://www.oliverwyman.com/content/dam/oliverwyman/v2/publications/2018/march/Large-Scale-Cyber-Attacks-DTCC-2018.pdf
- Internet Crime Complaint Center (IC3),Internet Crime Report, 2020,” FBI, USA, 2020.

Цахим эх сурвалж

- Эрх зүйн мэдээллийн нэгдсэн систем Legalinfo.mn
- Global Cybersecurity Index 2020 (itu.int)
- https://ncsi.ega.ee/country/mn_2022/?allData=1
- Үндэсний статистикийн хорооны цахим сан 1212.mn

АНХААРАЛ ХАНДУУЛСАНД БАЯРЛАЛАА

Судалгааны үзэл баримтлал, таамаглал

Судалгааны үзэл баримтлал:
Энэхүү судалгааны үзэл баримтлал нь “технологи хүлээн авах” загвар дээр суурилсан (Дэвис, 1989).

Судалгааны үр дүнд бий болсон загвар нь фишинг, хувийн мэдээллийг хулгайлах, хакердах зэрэг гурван үл хамаарах хувьсагч, цахим банкны хэрэглээ гэсэн нэг хамаарах хувьсагчаас бүрдэнэ.

Судалгааны таамаглал:

- ***Фишинг нь цахим банкны үйлчилгээнд сөргөөр нөлөөлнө***
- ***Хувийн мэдээллийг хулгайлах нь цахим банкны үйлчилгээнд сөргөөр нөлөөлнө***
- ***Хакердах нь цахим банкны үйлчилгээнд сөргөөр нөлөөлнө.***

2021.12.17

КИБЕР АЮУЛГҮЙ БАЙДЛЫН ТУХАЙ ХУУЛЬ

2021.12.28

Кибер аюулгүй байдлын үндэсний стратеги

2023.02.01

Кибер аюулгүй байдлын зөвлөлийн дүрэм, Кибер аюулгүй байдлын зөвлөлийн ажлын албаны ажиллах журам

2023.06.07

Кибер аюулгүй байдлыг хангах нийтлэг журам

2023.08.30

Кибер халдлага, зөрчилтэй тэмцэх үндэсний төвийн дүрэм, төвийн ажиллах журам

Кибер халдлага, зөрчилтэй тэмцэх нийтийн төв" улсын төсөвт үйлдвэрийн газрын дүрэм, байгууллагын бүтэц

ЦАХИМ ГЭМТ ХЭРГИЙН БАНКНЫ САЛБАРТ ҮЗҮҮЛЭХ НӨЛӨӨ

Санхүүгийн алдагдал, үйл ажиллагааны доголдол

Санхүүгийн шууд алдагдал: Санхүүгийн алдагдал нь банкны нэр хүнд болон харилцагчийн итгэлийг алдагдуулдаг. Accenture-аас саяхан хийсэн судалгаагаар цахим гэмт хэргийн хохирогч болсон банкны харилцагчдын 36 хувь нь банкандаа итгэх итгэлээ алдсан болохыг тогтоожээ. Эдгээр үйлчлүүлэгчдийн 65% нь “цахим банкны үйлчилгээнээс татгалзах болно” гэж мэдэгджээ.

Хэрэглэгчийн итгэл, нэр хүндэд учирсан хохирол

Банкны салбарын цахим гэмт хэргийн хамгийн чухал нөлөөллийн нэг нь үйлчлүүлэгчдийн санхүүгийн байгууллагуудад итгэх итгэл алдагдах явдал юм. Үйлчлүүлэгчид хувийн болон санхүүгийн мэдээллээ хамгаалахын тулд банкинд найддаг бөгөөд итгэлийг алдах нь тухайн байгууллагын нэр хүндэд сөргөөр нөлөөлж болзошгүй. Кибер гэмт хэргээс айж болгоомжлох явдал нь боломжит үйлчлүүлэгчдийг банкны үйлчилгээг ашиглахаас татгалзуулж, орлогын алдагдалд хүргэдэг.

	Initial	Extraction
CCT1	1.00	.874
CCT2	1.00	.698
CCT3	1.00	.843
CCT4	1.00	.831
CCT5	1.00	.754
CCT6	1.00	.794
CCT7	1.00	.776
BD1	1.00	.721
BD2	1.00	.783
BD3	1.00	.795
BD4	1.00	.668
BD5	1.00	.769
BD6	1.00	.799
OBU1	1.00	.751
OBU2	1.00	.793
OBU3	1.00	.851
OBU4	1.00	.718
OBU5	1.00	.811
OBU6	1.00	.741
OBU7	1.00	.700

Extraction Method: Principal Component Analysis.

Хэрэв хүчин зүйл нь хувьсагчдыг дэмжиж, хангалттай нийцтэй байвал түүнийг хүчин зүйлийн шинжилгээ ашиглан судалдаг. Хүчин зүйлийн уялдаа холбоог CCT (Цахим гэмт хэргийн арга техник, Cybercrime Techniques) болон BD (Онлайн банкны хэрэглээ, Online Banking Usage) тус тус 0.6-0.7 хооронд хэлбэлзэж байгаагаас харж болно. 0.7-0.8 утгын хүрээ нь хүчин зүйлийн шинжилгээнд OBU-г авч үзэхэд тохиромжтой юм. Эдгээр үр дүн нь нийлээд судалгааны арга болон фишинг, хувийн мэдээллийг хулгайлах, хакердах зэрэг үндсэн бүтцийн үнэн зөв байдлыг илтгэдэг..

шинжилгээний хэсэг

Хүснэгт 2. Дискриптив статистик

Давтамж, хэмжилтийн зүйл, дундаж утга, стандарт хазайлт зэргийг ашиглан өгөгдлийг нэгтгэн дүгнэвэл, кибер гэмт хэргийн дундаж утгыг 2.8-3.5, стандарт хазайлт 0.7-1, онлайн банкны хэрэглээний дундаж утга 4.0 байна.

Дундаж: Хувьсагч бүрийн дундаж оноог илэрхийлнэ. Жишээлбэл, фишингийн дундаж нь 3.2 байгаа нь судалгаанд оролцогчид фишинг халдлагад өртсөн туршлагаа 1-ээс 5 хүртэлх оноогоор дунджаар 3.2-оор үнэлсэн болохыг харуулж байна.

Стандарт хазайлт: Дундаж орчмын онооны тархалт эсвэл хэлбэлзлийг хэмждэг. Илүү өндөр стандарт хазайлт нь нэгэн төрлийн бус хариултууд ихээр ирсэн болохыг илтгэдэг. Жишээлбэл, фишингийн хувьд стандарт хазайлт 0.9 байгаа нь фишингийн туршлагын талаарх хариултууд дунджаар 3.2 онооны ойролцоо хэлбэлзэж байна гэсэн үг юм.

Variable	Mean	Standard Deviation
Phishing	3.2	0.9
Identity Theft	2.8	0.7
Hacking	3.5	1.0
E-banking Usage	4.0	0.6

Эх сурвалж: (Судлаачийн тооцоолол 2024)