МОНГОЛБАНК
САНХҮҮГИЙН МЭДЭЭЛЛИЙН АЛБА

Цахим залилангаас урьдчилан сэргийлэх хүчин зүйлсийн судалгаа ба вебд суурилсан шийдэл

МОНГОЛ БАНКНЫ САНХҮҮГИЙН МЭДЭЭЛЛИЙН АЛБАНЫ ЭРДЭМ ШИНЖИЛГЭЭНИЙ БҮТЭЭЛИЙН УРАЛДААНД ЗОРИУЛАВ

Удирдагч багш: Э. Тамир /Ph.D/

Гүйцэтгэсэн: О. Хонгорзул /СЭЗИС, Санхүү IV-р курс/
Э. Нямдаваа /СЭЗИС, Санхүү IV-р курс/
У. Бямбажав /МУИС, Эдийн засаг III-р курс/

АГУУЛГА

01

Удиртгал

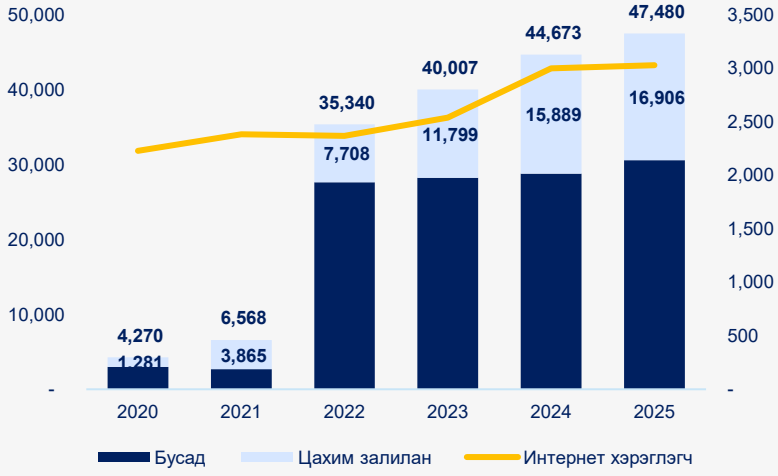
Судалгааны зорилго

Онол

Судлагдсан байдал

Судалгааны удиртгал

Бүртгэгдсэн залилангийн хэмжээ, Интернэт хэрэглэгчдийн тоо /сая/



Эх сурвалж: Цагдаагийн ерөнхий газар

Бүртгэгдсэн нийт хэрэг, хохирлын хэмжээ /2025/

2025 оны хохирлын хэмжээ: 592,836

Судалгааны зорилго

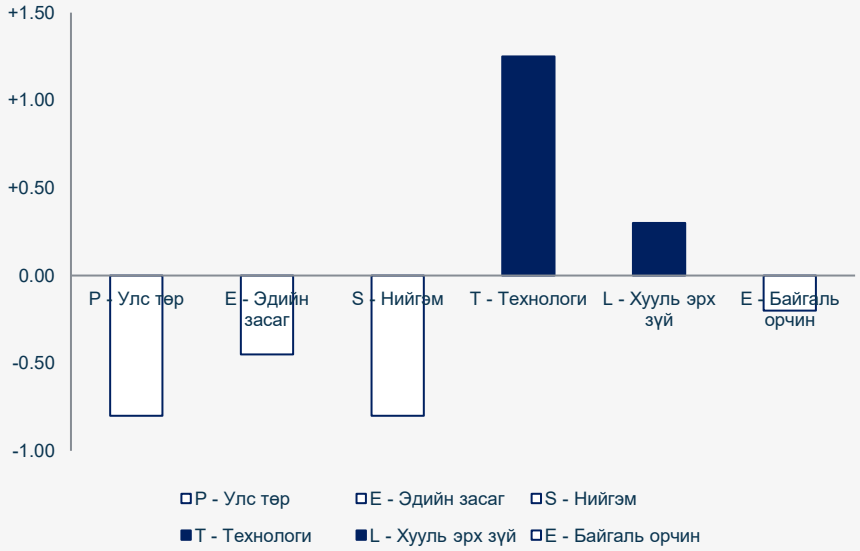
Цахим залиланг илрүүлэх, урьдчилан сэргийлэхэд чиглэсэн сургалт, хүний хүчин зүйл болон шинжилгээний аргуудын үр нөлөөг үнэлж, оновчтой шийдлийг тодорхойлох.

Pestle шинжилгээ

Үр дүн

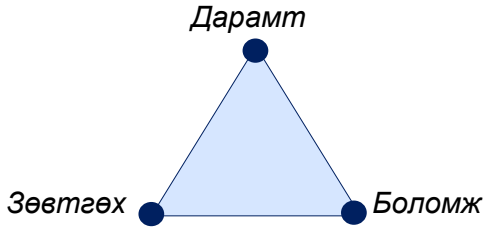
Хүчин зүйл	Ач холбогдол (A)	Нөлөөлөл (B)	Нийт (A x B)
P - Улс төр	0.20	-4	-0.80
E - Эдийн засаг	0.15	-3	-0.45
S - Нийгэм	0.20	-4	-0.80
T - Технологи	**0.25**	**5**	**+1.25**
L - Хууль эрх зүй	0.10	3	+0.30
E - Байгаль орчин	0.10	-2	-0.20
НИЙТ БАЙДАЛ	1.00		-0.70

Эх сурвалж: Судлаачийн тооцоолол



Pestle шинжилгээний үр дүнгээр Монгол Улсад цахим залилангаас урьдчилан сэргийлэх хамгийн өндөр боломж бүхий хүчин зүйл нь технологи байсан.

Залилан яагаад үйлдэгддэг вэ? 01



Сэтгэлзүйд нөлөөлж, мөнгө болон мэдээлэл авах цахим залилан.

Ямар нөхцөл бүрдвэл залилан үйлдэгддэг вэ? 02

- *Тохиромжтой бай*
- *Сэдэл бүхий этгээд*
- *Хамгаалалтын орчин сул байх*

Ямар арга заль хэрэглэдэг вэ? 03

Нэр хүндтэй байгууллага, хүний дүрд орох
Яаруулах
Хоцорч буй мэт мэдрэмж төрүүлэх

Хүмүүс яагаад залилуулдаг вэ? 04

Өөртөө хэт итгэх
Боломжийг алдчих вий гэсэн айдас
Баталгаажуулалгүй шууд итгэх

Судлагдсан байдал

Цахим залилангийн эсрэг тогтолцоо

Дэлхий нийт технологи, хууль эрх зүй, институтийн бүтэц болон олон улсын хамтын ажиллагаа гэсэн гурван тулгуурт суурилсан стратеги баримталдаг.

Уг 3 тулгуур бие биеэ дэмжиж, хоорондоо зөрчилдөхгүй байх хэрэгтэй.

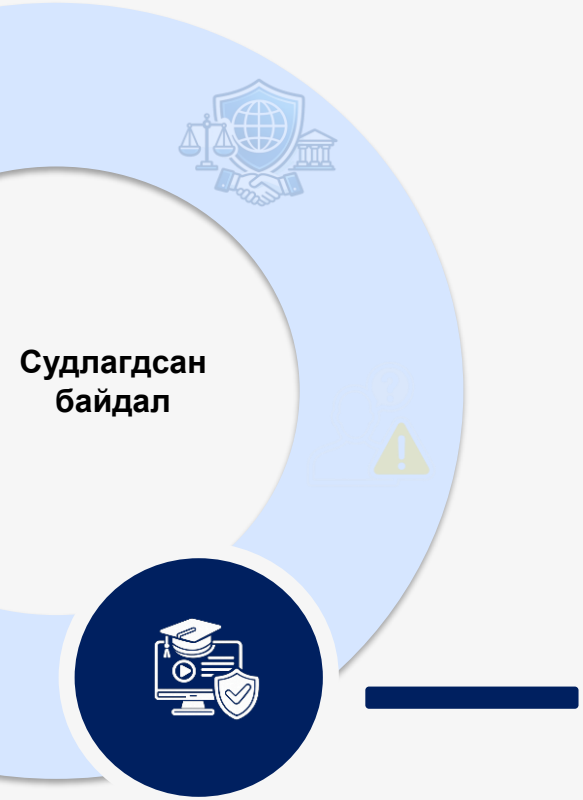
Судлагдсан байдал

Цахим залиланд өртөх шалтгаан

Витти, М. Т. (2018) : Хүмүүсийн сэтгэл зүй

Пратт, Трэвис С. нар (2019): Цахим орчин дахь хамгаалах хяналт, мэдлэг, сэрэмж хангалтгүй байх

Дхамия,Р. нар (2021) : Аюулгүй байдлын талаарх мэдлэг дутмаг байх



Цахим залилангаас урьдчилан сэргийлэх хамгийн үр дүнтэй арга

Шэнг нар (2017), Канова нар (2015) : Интерактив байх, хүмүүсийг өөрсдийг нь сургалтад оролцуулсан сургалт

Кумагару нар (2019) : Сургалтын дараа юун дээр алдсаныг нь шууд хэлэх

Саамер нар (2022), Аяола нар (2024) : Сургалт

Аллукмани нар (2025) : Нэг удаагийн сургалт хангалтгүй, харин давтамжтай, ялангуяа бодит нөхцөл байдлын дуурайсан сургалт

02

Үндсэн хэсэг

Арга зүй

Тоон шинжилгээ

Чанарын шинжилгээ

Симуляцид суурилсан сургалтаа туршсан

Тоон шинжилгээ

Өгөгдөл цуглуулах
- *Урьдчилсан туршилт*
- *Найдвартай байдал*
- *Дахин өгөгдөл цуглуулах*

→ **Өгөгдөл бэлтгэх** → **Шинжилгээ**

Чанарын шинжилгээ

Цахим залилангийн эсрэг платформуудыг үр дүнгээр нь харьцуулан үнэлсэн.

- *Асуултууд хоорондоо логик уялдаатайгаар бүлэглэгдэж буй эсэх* → Хүчин зүйлийн шинжилгээ
- *Асуулгууд нэг ойлголтыг зөв хэмжиж байгаа эсэхийг баталгаажуулах.* → Найдвартай байдлын шинжилгээ
- *Хүчин зүйлс болон залиланд өртсөн эсэхийн хамаарлыг тодорхойлсон.* → Хамаарлын шинжилгээ
- *Хүчин зүйлс залиланд өртөх магадлалд хэрхэн нөлөөлж байгааг үнэлсэн.* → Ложистик регресс

→ **Үр дүн**

Өгөгдөл таницуулга

Судалгааны өгөгдөл

Судалгаанд цахим залиланд өртөмтгий байдал болон урьдчилан сэргийлэх зан чанарыг тодорхойлох **6 хүчин зүйл, 18 тайлбарлагч ашигласан**. Хувьсагчдыг 5 шатлалтай Ликертийн хуваарь ашиглан хэмжсэн.

Хувьсагчдыг Alluqmani (2025), Greitzer et al. (2021), Ribeiro at al. (2024), Sumner at al (2021): Нийт 504 хүн оролцсон.

Зан чанар

Итгэмтгий байдал, эрсдэл хүлээх сонирхол, түргэн шийдвэр гаргах хандлага.

Мэдлэг

Цахим залилангийн арга, хувийн мэдээллийн нууцлалын талаарх ойлголт.

Мэдээлэл

Залилангийн талаарх сэрэмжлүүлэг, албан эх сурвалжаас мэдээлэл авсан.

Технологи

2FA, Хүчтэй нууц үг, төхөөрөмжийн аюулгүй байдал тохиргоо ашиглах.

Сэтгэл зүй

Айдас, сандрал, яаруулах, өрөвдөх сэтгэлд автах байдал.

Урьдчилан сэргийлэх

Гүйлгээ шалгах, дансны хуулга хянах, бусдад зөвлөгөө өгөх зан үйл.

Шинжилгээний үр дүн

Хамаарлын шинжилгээ

Хүчин зүйлс	Зан чанар	Мэдлэг	Мэдээлэл	Технологи	Сэтгэл зүй	Сэргийлэх арга
Зан чанар	1					
Мэдлэг	-.343**	1				
Мэдээлэл	.007	**-.033**	1			
Технологи	.576**	**-.505****	.168**	1		
Сэтгэл зүй	.570**	**-.500****	.061	.658**	1	
Сэргийлэх арга	.597**	**-.568****	.067	**.698****	**.731****	1

Эх сурвалж: Судлаачийн тооцоолол

Ложистик шинжилгээ

Хүчин зүйлс	B	S.E.	Wald	df	Sig.	Exp(B)
Итгэлцэл (Trust)	**1.976**	**0.266**	**55.277**	**1**	**0.000**	**7.216**
Мэдлэг (Knowl)	**-0.885**	**0.231**	**14.676**	**1**	**0.000**	**0.413**
Мэдээлэл (Info)	0.167	0.173	0.926	1	0.336	1.182
Технологи (Tech)	**0.801**	**0.226**	**12.608**	**1**	**0.000**	**2.229**
Сэтгэл зүй (Psy)	0.078	0.242	0.105	1	0.746	1.082
Урьдчилан сэргийлэлт (Prev)	**0.840**	**0.268**	**9.831**	**1**	**0.002**	**2.316**
Constant	-8.668	1.307	44.004	1	0.000	0.000

Эх сурвалж: Судлаачийн тооцоолол

Цахим залиланд өртөх нөлөө

Цахим залиланд өртөхөд нөлөөлдөг хүчин

Итгэлцэл (Зан чанар)

*Хамгийн хүчтэй нөлөөтэй хүчин зүйл. Хэрэглэгч бусдад амархан итгэх, сэжиглэхгүй байх тусам цахим залиланд өртөх магадлал **7.2 дахин нэмэгдэж** байна.*

Мэдлэг

Сөрөг нөлөөтэй хүчин зүйл. Цахим аюулгүй байдлын мэдлэг нэмэгдэх тусам залиланд өртөх эрсдэл буурч байна.

Технологи

Технологийн хэрэглээ статистикийн ач холбогдолтой гарсан. 2FA, хүчтэй нууц үг, аюулгүй байдлын тохиргоо ашиглах чадвар нь цахим орчин дахь эрсдэлийг танихад чухал нөлөө үзүүлж байна.

Урьдчилан сэргийлэх

Урьдчилан сэргийлэх идэвхтэй зан үйл нь ач холбогдолтой гарсан. Гүйлгээ шалгах, дансны хуулга хянах зэрэг дадал нь цахим залилангаас хамгаалахад чухал нөлөөтэй байна.

ЧАНАРЫН ШИНЖИЛГЭЭНИЙ ХЭСЭГ

Кибер хамгаалалтын платформуудын харьцуулалт

СУДАЛСАН ПЛАТФОРМУУД

KnowBe4

- Зан төлөвийн шинжилгээ
- Пишинг симуляци
- Хувь хүнд тохирсон сургалт
- Динамик сургалтын контент

proofpoint.

- Машин сургалт
- Имэйлийн аюул илрүүлэлт
- Автомат хариу арга хэмжээ

COFENSE

- Фишинг таних
- Аюулыг ангилах автоматжуулалт
- Хариу арга хэмжээний урсгал

HOXHUNT

- Тоглоомжуулсан сургалт
- Оноо ба урамшуулал
- Дасан зохицох сургалт

ШИНЖИЛГЭЭНИЙ ГОЛ ҮР ДҮН

1

AI + ХҮНИЙ ЗАН ТӨЛӨВ

Хамгийн үр дүнтэй

2

ТОГЛООМЧИЛСОН СУРГАЛТ

Оролцоог нэмэгдүүлдэг

3

ҮҮЛЭН ТЕХНОЛОГИ

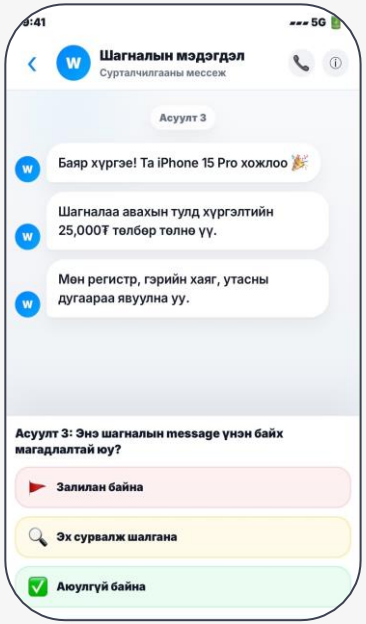
Хамтын хамгаалалтыг дэмждэг

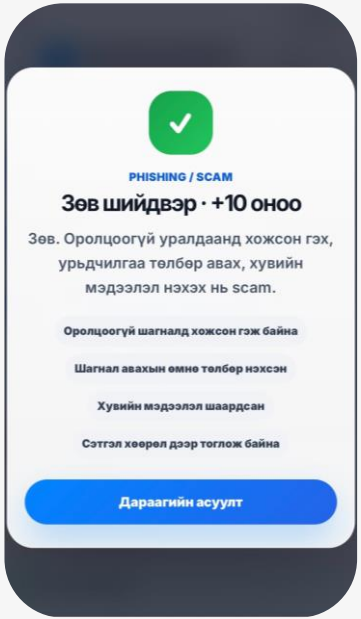
СИМУЛЯЦИД СУУРИЛСАН СУРГАЛТАА ТУРШСАН

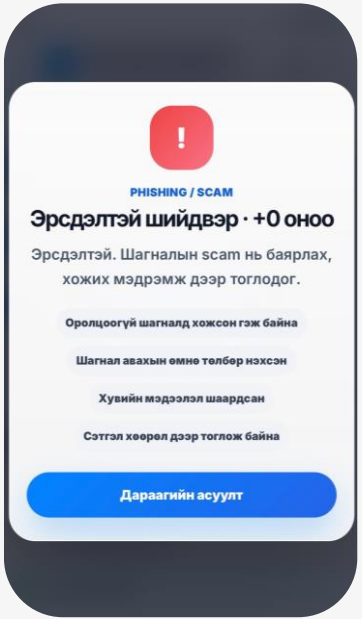
105 ахмад настан

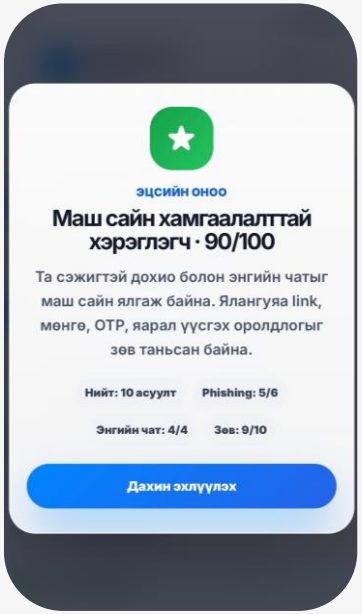
20 минутад 10 мессежүүдэд хариу өгөх

Хариу өгсний дараа шууд үр дүн харагдана









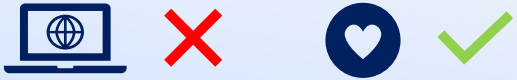
Идэвхтэй оролцоо ба хандлага

Чадварын ахиц

03

Дүгнэлт

Юун дээр тулгуурлаж залилан үйлдэгддэг вэ?



Технологи биш, хүний сэтгэл зүй

Урьдчилан сэргийлэхэд нөлөөлөх хүчин зүйлсийн эрэмбэ

Урьдчилан сэргийлэх стратеги= технологи

04

Ном зүй

1. Pratt, T. C., Holtfreter, K., & Reisig, M. D. (2010). Routine online activity and internet fraud targeting: Extending the generality of routine activity theory. Journal of Research in Crime and Delinquency, 47(3), 267–296.s
2. Leukfeldt, E. R. (2014). Phishing for suitable targets in the Netherlands: Routine activity theory and phishing victimization. Cyberpsychology, Behavior, and Social Networking, 17(8), 551–555.
3. Ngo, F. T., & Paternoster, R. (2011). Cybercrime victimization: An examination of individual and situational level factors. International Journal of Cyber Criminology, 5(1), 773–793.
4. Whitty, M. T. (2013). The scammers persuasive techniques model: Development of a stage model to explain scam compliance. British Journal of Criminology, 53(4), 665–684.
5. Dhamija, R., Tygar, J. D., & Hearst, M. (2006). Why phishing works. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (pp. 581–590). ACM.
6. Ribeiro, L., Guedes, I. S., & Cardoso, C. S. (2024). Which factors predict susceptibility to phishing? An empirical study. Computers & Security, 136, 103558. https://doi.org/10.1016/j.cose.2023.103558
7. Alluqmani, K., Karrar, A. E., Alhaidari, M., Alharbi, R., & Alharbi, S. (2025). Assessing the efficacy of security awareness training in mitigating phishing attacks: A review. International Journal of Advanced Trends in Computer Science and Engineering, 14(3), 177–184. https://doi.org/10.30534/ijatcse/2025/081432025
8. Ayoola, V. B., James, U. U., Idoko, P. I., Ijiga, M. I., & Olola, T. M. (2024). Effectiveness of social engineering awareness training in mitigating spear phishing risks in financial institutions from a cybersecurity perspective. Global Journal of Engineering and Technology Advances, 20(3), 94–117. https://doi.org/10.30574/gjeta.2024.20.3.0164
9. Sumner, A., Yuan, X., Anwar, M., & McBride, M. (2022). Examining factors impacting the effectiveness of anti-phishing trainings. Journal of Computer Information Systems, 62(5), 975–997. https://doi.org/10.1080/08874417.2021.1955638
10. Greitzer, F. L., Li, W., Laskey, K. B., Lee, J., & Purl, J. (2021). Experimental investigation of technical and human factors related to phishing susceptibility. ACM Transactions on Social Computing, 4(2), Article 8. https://doi.org/10.1145/3461672
11. Arachchilage, N. A. G., Tarhini, A., & Love, S. (2016). Designing a mobile game to thwart malicious IT threats: A phishing threat avoidance perspective. *Computers in Human Behavior*, 63, 173–192.
12. Canova, G., Volkamer, M., Bergmann, C., & Borza, R. (2015). NoPhish: An anti-phishing education app. In *Proceedings of the 11th Symposium on Usable Privacy and Security (SOUPS 2015)* (pp. 223–238).
13. Kumaraguru, P. (2009). *PhishGuru: A system for educating users about semantic attacks* (Doctoral dissertation, Carnegie Mellon University). ProQuest Dissertations & Theses.
14. Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L. F., Hong, J., & Nunge, E. (2007). Anti-phishing Phil: The design and evaluation of a game that teaches people not to fall for phish. In *Proceedings of the 3rd Symposium on Usable Privacy and Security (SOUPS 2007)* (pp. 88–99). ACM.
15. The Impact of Cybercrime on Security in Africa: A Case Study of Côte d'Ivoire. (2026). Retrieved from https://asjp.cerist.dz/en/article/286747
16. Enhancing credit card fraud detection with a stacking-based hybrid machine learning approach. (2025). *PeerJ Computer Science*. https://doi.org/10.7717/peerj-cs.3007
17. Fraud Risk and Audit Opinions Across Countries: Complementing Accounting-Based Fraud Risk with Machine Learning Methods. (2025). Journal of Risk and Financial Management Retrieved from https://www.mdpi.com/1911-8074/19/1/26
18. Online Financial Fraud and the Role of Financial Technology in Mitigation. (n.d.). *Journal of Management Sciences and Research Review*. Retrieved from https://www.jmsrr.com/index.php/Journal/article/view/435/389
19. Fraud Detection in Mobile Payment Systems using an XGBoost-based Framework. (2022). *Information Systems Frontiers*. https://doi.org/10.1007/s10796-022-10346-6

МОНГОЛБАНК
САНХҮҮГИЙН МЭДЭЭЛЛИЙН АЛБА

АНХААРАЛ ХАНДУУЛСАНД БАЯРЛАЛАА