International Journal of Social Science and Humanities Research-MIYR

ISSN(print): 2788-9092 ISSN(Online): 2788-9106

Volume 5. Issue 2. 2025.06

The impact of information technology skills on cyber deviance among employees in the banking sector of Mongolia

Narantungalag Ganbat • Gerelmaa Damba • Nandin-Erdene Banzragch • Delgersaikhan Bold • Tamir Enkhbat

MISHEEL
INSTITUTE FOR YOUNG RESEARCHERS

International Journal of Social Science and Humanities Research-MIYR
Volume 5, Issue 2, pp.1~20, 2025
ISSN(print): 2788-9092, ISSN(Online): 2788-9106
https://youngres.com https://doi.org/10.53468/mifyr.2025.05.02.01

The impact of information technology skills on cyber deviance among employees in the banking sector of Mongolia

Narantungalag Ganbat[1], Gerelmaa Damba[2*], Nandin-Erdene Banzragch[3], Delgersaikhan Bold[4], Tamir Enkhbat[5]

[1,2,5]*Business Management Department, University of Finance and Economics, Mongolia*
[1]narantungalag.g@ufe.edu.mn, [2]gerelmaa.d@ufe.edu.mn, [5]tamir.en@ufe.edu.mn
[3]*Marketing Management Department, University of Finance and Economics, Mongolia*
[3]nandinerdene.b@ufe.edu.mn
[4]*Accounting Department, University of Finance and Economics, Mongolia*
[4]delgersaikhan.b@ufe.edu.mn

Abstract - The rapid digitalization of the banking sector has significantly increased employees' reliance on information technology (IT), thereby creating new opportunities for various forms of cyber deviance in the workplace. This study aimed to investigate the relationship between employees' IT skill levels and the occurrence of cyber deviance among bank employees. The study was conducted in the Mongolian banking sector, which has undergone substantial digital transformation in recent years. A quantitative research design was employed, and a total of 434 bank employees participated in the study. Data were collected using a validated 24-item survey instrument measuring four dimensions of cyber deviance: unauthorized IT access, cyberslacking, computer abuse, and cyberaggression. To ensure the robustness of the measurement model, exploratory factor analyses were conducted, followed by one-way analysis of variance (ANOVA) to examine differences in cyber deviance across varying levels of IT skills. The results showed that employees' IT skill levels did not have a statistically significant effect on the overall frequency of cyber deviance. However, a notable finding was that employees with advanced IT skills reported a higher tendency to monitor their coworkers' computer usage. This suggests that higher technical proficiency may be associated with informal surveillance behaviors rather than direct engagement in cyber deviance. These findings indicate that cyber deviance in banks cannot be explained solely by employees' technical capabilities but should be understood within a broader organizational and ethical context. The study highlights the importance of developing targeted cybersecurity policies, ethical guidelines, and training programs that address both overt and subtle forms of cyber deviance. By focusing on employee awareness, supervision practices,

Received: 2025.03.25
Reviewed: 2025.03.27
Accepted: 2025.05.03
*Corresponding author: Gerelmaa Damba

and ethical IT use, this research provides practical insights for enhancing organizational security and governance in digitally transforming banking institutions.

Keywords - Cyber deviance, IT skills, workplace behavior, banking sector, Mongolia

1. INTRODUCTION

The advancement of information technology (IT) has brought significant positive changes to both professional and personal life. However, it has also introduced risks related to inappropriate and unethical usage [1], [2], [3], [4], [5] In today's workplace, information and communication technology (ICT) is widely used, enabling seamless remote work and fundamentally transforming organizational operations [6], [7], [8] . As a result, technology has become an indispensable tool in professional and social life, leading organizations to develop and implement IT-related management policies. [9]

With the rapid evolution of technology, deviant workplace behaviors traditionally studied within organizational behavior research have increasingly shifted into the digital realm. As new forms of cyber deviance continue to emerge, measuring and understanding these behaviors has become crucial. Akanksha Malik, Shuchi Sinha, and Sanjay Goel (2021) conducted a qualitative review of 245 scholarly articles on workplace deviance published between 2003 and 2020 in their study, *"Qualitative Review of 18 Years of Research on Workplace Deviance: New Vectors and Future Research Directions"*. Their findings highlight that workplace deviance remains a pressing issue for organizations, and existing definitions must be expanded to incorporate emerging forms of deviance in digital environments [10] Furthermore, technological advancements not only facilitate invisible and easily executed cyber deviant behaviors but also make their detection increasingly difficult. The study also suggests that IT skills could be a contributing factor to the likelihood of engaging in cyber deviance.

The continuous connectivity to workplace IT systems can lead to psychological stress and loss of control among employees [11], while also negatively affecting organizational productivity as employees spend work hours on personal activities. [12] Additionally, cyber deviant behaviors pose multiple risks to organizations, including damage to corporate reputation, financial losses [13], data security breaches, and diminished client trust. Thus, understanding the frequency and impact of workplace cyber deviance and formulating management policies for prevention and mitigation is essential.

The banking sector in Mongolia plays a crucial role in the country's financial system and has been undergoing rapid digital transformation in recent years. As banking services shift towards digital platforms, employees' work responsibilities are increasingly integrated into online environments. Consequently, managing and adapting to behavioral changes in the workplace has become necessary. [14]

Despite the growing need to study cyber deviant behaviors in employees, limited research exists in this area, particularly in Mongolia. This research aims to adapt and examine theoretical concepts of cyber deviance within the Mongolian banking sector, measuring the frequency of cyber deviance among employees. The study's findings will help develop IT usage regulations,

enhance organizational monitoring strategies, and improve employee productivity in banking institutions.

Research Objective

This study aims to develop a research design based on existing theoretical frameworks of cyber deviance, its classification, and measurement methodologies, followed by empirical research on employees in Mongolia's banking sector to derive findings and recommendations.

Research Objectives

- To provide a literature review on cyber deviance, its classifications, and measurement methodologies.
- To conduct empirical research in the Mongolian banking sector and draw key findings.
- To develop recommendations for preventing cyber deviant behaviors among employees.

Research Questions

- What is the current level of cyber deviance among employees in Mongolia's banking sector? [8]
- How do IT skill levels influence employees' engagement in cyber deviances? [8], [15]

1. LITERATURE REVIEW

1.1 Employee Cyber Deviance

Since the 1990s, the rapid development of information and communication technology (ICT) has transformed the traditional concept of the workplace, expanding it beyond physical locations to include virtual work environments. As a result of this transformation, the term "cyber deviance" has emerged as a research concept to describe workplace misconduct related to digital technology.

Several scholars have provided different definitions of cyber deviance:

Holt & Bossler (2016) define it as "illegal, unethical, or morally ambiguous behaviors associated with the use of computer systems and networks," which includes hacking, cybercrimes, online harassment, and cyberbullying.

Yang (2022) describes cyber deviance as "any non-normative, non-compliant, or inappropriate behavior that violates organizational policies and ethical standards in cyberspace."

Although there is no universally agreed definition of employee cyber deviance, it is generally understood as actions that violate social norms or legal regulations, occurring through the misuse of digital technology.

1.2 Cyber Deviance in the Workplace

Various studies have examined cyber deviance in relation to workplace environments, offering different perspectives on how it manifests:

The workplace is an environment where employees perform job-related tasks using ICT, and the misuse of these technologies can negatively impact organizational operations. Examples include using company resources for personal needs, cyberattacks, fraud, and sabotage[13]

The workplace is a setting where employees utilize IT to achieve organizational goals; however, inappropriate use of IT within this setting violates corporate rules and ethics. Employees' non-compliance with explicit and implicit organizational norms can harm both the organization and individual employees [16]

The workplace is a structured environment where IT usage is expected to align with organizational regulations, yet some employees use work hours for personal activities, negatively affecting productivity [17]

The workplace is an environment where employees utilize corporate resources, but inappropriate use of the internet and IT negatively impacts productivity. [12]

The workplace is an environment where employees must adhere to organizational rules and work efficiently. However, the misuse of technology disrupts workplace culture and reduces productivity. Cyber deviance includes illegal activities, deliberate damage to organizational resources, and misuse of IT for personal gain [6].

The workplace is a collaborative environment, but the anonymous and accessible nature of the internet influences employee behavior, presenting new challenges for organizations. Cyber deviance includes cyber harassment, cyberattacks, and fraud, yet existing regulatory mechanisms remain insufficient. [18]

"In summary, the workplace is an environment where employees utilize information and communication technology (ICT) to perform job-related tasks in alignment with organizational goals, adhering to company policies, utilizing corporate resources, and collaborating with colleagues. However, employee cyber deviance refers to behaviors that occur within the organization's digital environment, where IT resources are used in violation of organizational policies and ethical standards, potentially harming the organization’s operations."

1.3 Key Characteristics of Employee Cyber Deviance

From the above perspectives, the workplace is defined as an environment where employees use ICT to fulfill organizational goals while adhering to policies, utilizing resources, and collaborating with colleagues. Employee cyber deviance refers to behaviors that violate organizational norms, ethical standards, and IT policies, potentially harming the organization.

According to [8], cyber deviance in the workplace exhibits the following key characteristics:

1) Intentionality – Cyber deviance involves deliberate actions rather than accidental misuse of IT resources. Unintentional errors are not considered cyber deviance.
2) Behavior-Oriented Definition – Cyber deviance is defined based on how technology is used, rather than the intent behind the actions. Harmful intent is not a requirement; the

primary concern is whether IT resources are used outside of organizational norms and policies.

3) Employee's actions – Cyber deviance focuses on the misuse of IT by internal employees rather than external hackers or unauthorized third parties.
4) Internal Organizational Focus – The study of cyber deviance is limited to workplace misconduct within the organization, excluding actions directed toward external stakeholders.

1.4 Typology of employee cyber deviance

To identify common types of cyber deviance in the workplace, develop a multidimensional scale for measurement, classify these behaviors, and establish appropriate terminology, researchers Srinivasan Venkatraman, Christy M. K. Cheung, Zach W. Y. Lee, Fred D. Davis, and Viswanath Venkatesh conducted a comprehensive three-phase study in 2018 [8].

This study validated a three-dimensional typology of employee cyber deviance, which includes the following dimensions:

1) Minor versus serious
2) Individual versus organizational
3) Low technical skill versus high technical skill

Table 1 presents examples of common cyber deviances based on this classification framework.

This study contributes to the development of a systematic typology of employee cyber deviance, establishing a theoretical foundation that enables researchers to examine the interrelationships between different deviant behaviors. Previously, many deviant behaviors were studied individually, but this research provides a comprehensive framework to analyze multiple forms of misconduct simultaneously.

1.5 Measurement of Cyber Deviance: Four Key Factors

The study identified and measured four key dimensions of cyber deviance:

Unauthorized Access and Use of IT

Unauthorized usage of an organization's IT resources is considered a minor but organizational deviance that requires high levels of IT skill [8].

Cyberslacking (Cyberloafing)

Cyberslacking refers to the use of IT for non-work-related purposes. It is classified as a behavior organizational, requiring low levels of IT skills, and may range from minor misconduct to serious violations [8]. These behaviors have been widely studied within the field of organizational behavior. Additionally, cyberslacking is linked to productivity loss (as it reduces work efficiency) and resource misuse (as it consumes organizational internet bandwidth and IT infrastructure).

Computer Abuse

Computer abuse involves the misuse of IT related to cybersecurity, privacy breaches, and fraud. This type of cyber deviance is organizational, requires high levels of IT skills, and is associated

with serious harm [19]. These behaviors have been extensively explored in information systems research.

Cyberaggression:

Cyberaggression refers to cyber harassment, bullying, or aggressive behavior among employees. Unlike other types of cyber deviance, cyberaggression is individual and can require either low or high levels of IT skill [8]. Unlike other categories, cyberaggression has been scarcely examined in a systematic manner within information systems research.

2. RESEARCH DESIGN

This study examines the types of employee cyber deviance and their relationship with IT skill levels. The research design is visually represented in the following diagram.

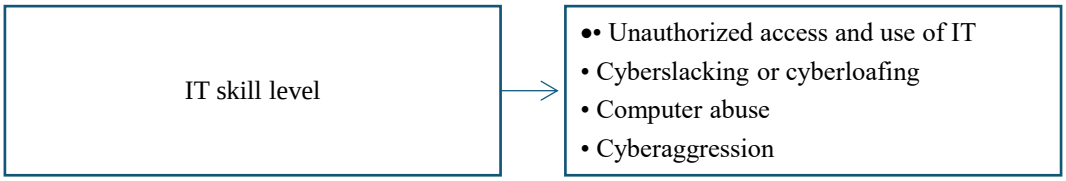

Figure 1 Research design

3.1 Research Hypothesis

H1: Higher IT skill is associated with an increased frequency of cyber deviant behaviors [8]

3.2 Scope and Methodology

This study employs a quantitative research approach and measures the frequency of cyber deviant behaviors among employees using the classification framework developed by Srinivasan Venkatraman, Christy M.K. Cheung, Zach W.Y. Lee, Fred D. Davis, and Viswanath Venkatesh. [8] Their framework includes 24 specific deviant actions, each evaluated using a 7-point Likert scale (1 = Never, 7 = Daily).

Data collection involved random sampling of 434 employees from commercial banks in Mongolia, ensuring representative coverage of the banking workforce. The data were collected between October 1, 2024, and February 27, 2025, allowing for an analysis of cyber deviant behavior frequencies in the context of real-time workplace conditions [14]

The study also assessed employees' IT proficiency levels to determine whether their skill levels influence engagement in cyber deviance. Data was collected via Qualtrics survey platform and face-to-face, followed by descriptive statistical analysis, reliability testing, factor analysis, and correlation analysis.

3.3 Research Sample

This study surveyed 434 employees from Mongolia's banking sector. The participants were selected based on three main criteria:

1) Currently employed in a commercial bank
2) At least one year of work experience in the banking sector
3) Full-time employees

3.4 Survey Instrument

The study measured the frequency of employee cyber deviance using a validated questionnaire developed by Srinivasan Venkatraman, Christy M.K. Cheung, Zach W.Y. Lee, Fred D. Davis, and Viswanath Venkatesh. This instrument consists of three dimensions, eight categories, and 24 questions designed to capture cyber deviant behaviors.

The selected questionnaire is based on internationally recognized classifications, ensuring their validity and applicability in environments where IT is heavily utilized. Given the digital nature of Mongolia's banking and financial sector, this instrument was deemed appropriate for measuring cyber deviance within the industry.

3.5 Data Collection Process

Data collection was conducted between October 1, 2024, and February 7, 2025. The survey was distributed to 606 participants, out of which 434 valid responses were analyzed.

3.6 Data analysis

Survey data collected online was extracted from the Qualtrics platform, while paper-based responses were manually coded and integrated into SPSS software for analysis. Statistical analyses were conducted using SPSS to ensure accuracy and reliability.

3.7 Ethical Considerations

The study adhered to strict ethical guidelines to ensure the protection and confidentiality of participants. The following ethical principles were upheld:

- Confidentiality – All personal information of participants was protected.
- Voluntary Participation – Participants joined the study on a voluntary basis.
- Informed Consent – The research purpose was clearly explained to participants in writing before participation.
- Anonymity – No personal identifiers such as names, organization details, or any traceable information were collected to protect individual and institutional identities.

3. RESULTS

4.1 IT Skill Levels

The study categorized IT skill into four common levels and provided a description for each level. The classification and the distribution of participants across these levels are presented in the following table.

Table 1 Distribution of Respondents by IT skill levels

IT skill levels	Frequency	Percentage
Basic level	29	6.70%
Intermediate Level	252	58.10%
Advanced Level	112	25.80%
Expert Level	41	9.40%

4.2 Descriptive Statistical Analysis

The mean and frequency distributions of cyber deviances are presented in the following tables.

3.1 Unauthorized access and use of IT

Table 2. Frequency of Unauthorized Access and Use of IT

Unauthorized access and use of IT	Mean	7	6	5	4	3	2	1
		Daily	Weekly	Monthly	Several times a year	Twice a year	Once a year	Never
Concealing identity online and deceiving co-workers	1.13	0.5%	0.2%	0.2%	1.2%	1.2%	2.5%	94.2%
Engaging in identity theft	1.15	0.2%	0.0%	0.2%	1.6%	1.6%	4.1%	92.2%
Unauthorized access to co-workers' computers	1.18	0.5%	0.0%	0.2%	2.8%	1.2%	3.7%	91.7%
Concealing identity and deceiving co-workers	1.18	0.7%	0.0%	0.9%	1.2%	1.4%	4.4%	91.5%

International Journal of Social Science and Humanities Research-MIYR
Volume 5, Issue 2, pp.1~20, 2025
ISSN(print): 2788-9092, ISSN(Online): 2788-9106
https://youngres.com https://doi.org/10.53468/mifyr.2025.05.02.01

3.2 Cyberslacking or cyberloafing

Table 3. Frequency of Cyberslacking Behaviors

Cyberslacking or cyberloafing	Mean	7 Daily	6 Weekly	5 Monthly	4 Several times a year	3 Twice a year	2 Once a year	1 Never
Playing computer games	1.45	1.6%	0.7%	1.4%	6.2%	1.8%	4.4%	83.9%
Smearing the company online	1.47	0.7%	0.2%	1.6%	5.1%	5.5%	8.5%	78.3%
Sending/receiving personal emails	1.58	0.7%	0.7%	1.6%	8.5%	3.5%	11.1%	74.0%
Engaging in computer rage	2.14	1.6%	2.3%	5.3%	15.2%	7.1%	11.3%	57.1%
Browsing away work time	2.43	5.1%	4.6%	4.1%	17.1%	5.8%	10.6%	52.8%

3.3 Computer abuse

Table 4. Frequency of Computer Abuse

Computer abuse	Mean	7 Daily	6 Weekly	5 Monthly	4 Several times a year	3 Twice a year	2 Once a year	1 Never
Encrypting company data and taking data hostage	1.06	0.5%	0.0%	0.0%	0.7%	0.5%	0.7%	97.7%
Spreading viruses in work computers	1.03	0.0%	0.0%	0.0%	0.2%	0.5%	1.6%	97.7%
Hacking and intrusion into computer resources	1.08	0.2%	0.0%	0.2%	0.5%	1.4%	1.2%	96.5%
Posting critical company information online	1.07	0.0%	0.0%	0.2%	0.5%	0.9%	2.5%	95.9%
Unauthorized installation of hardware and software in company computers	1.14	0.2%	0.0%	0.0%	1.8%	1.6%	3.5%	92.9%

3.4 Cyberaggression

Table 5. Frequency of Cyberaggression

Cyberaggression	Mean	7 Daily	6 Weekly	5 Monthly	4 Several times a year	3 Twice a year	2 Once a year	1 Never
Distributing pornography content to co-workers	1.07	0.0%	0.2%	0.2%	0.7%	0.7%	1.2%	97.0%
Distributing violent and hatred content online	1.09	0.2%	0.0%	0.2%	0.5%	1.4%	2.1%	95.6%
Sending spam and mass email messages	1.41	1.2%	1.4%	0.9%	4.4%	2.3%	5.8%	84.1%
Spreading rumors and gossip about co-workers electronically	1.50	0.9%	1.6%	1.4%	6.2%	3.0%	6.7%	80.2%

An integrated summary of the results presented in Tables 5 to 8 reveals the following key patterns regarding cyber deviance among employees:

- Cyberslacking emerged as the most frequently reported type of cyber deviance, indicating a widespread trend of personal internet use during work hours that may reduce productivity.
- Cyberaggression, primarily involving interpersonal misconduct such as rumor-spreading, was also observed, particularly in non-confrontational digital formats.
- Computer abuse, while less frequent, was more noticeable among employees with higher IT skill levels, suggesting a technical capability element to these actions.
- Unauthorized access and use of IT showed the lowest average frequency, yet this behavior presents the highest potential threat to organizational cybersecurity.

These findings underscore the need for targeted internal policies and employee training to mitigate the most prevalent and high-risk cyber deviance in the banking sector.

International Journal of Social Science and Humanities Research-MIYR
Volume 5, Issue 2, pp.1~20, 2025
ISSN(print): 2788-9092, ISSN(Online): 2788-9106
https://youngres.com https://doi.org/10.53468/mifyr.2025.05.02.01

4.3 Factor analysis

Table 6. Total Variance Explained

Total Variance Explained							
Component	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings[a]
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total
1	6.606	36.698	36.698	6.606	36.698	36.698	4.985
2	1.683	9.353	46.050	1.683	9.353	46.050	4.257
3	1.421	7.892	53.942	1.421	7.892	53.942	3.966
4	1.219	6.772	60.714	1.219	6.772	60.714	4.041
5	0.933	5.184	65.898				
6	0.864	4.800	70.698				
7	0.718	3.988	74.686				
8	0.644	3.580	78.266				
9	0.545	3.027	81.293				
10	0.512	2.846	84.139				
11	0.474	2.633	86.772				
12	0.458	2.544	89.316				
13	0.379	2.104	91.420				
14	0.365	2.029	93.449				
15	0.350	1.946	95.395				
16	0.326	1.812	97.207				
17	0.306	1.698	98.905				
18	0.197	1.095	100.000				
Extraction Method: Principal Component Analysis.							
a. When components are correlated, sums of squared loadings cannot be added to obtain a total variance.							

Factor analysis was conducted using the Principal Component Analysis (PCA) method. The results indicate that the first four factors had Eigenvalues greater than 1, collectively explaining 60.7% of the total variance. In social sciences and behavioral research, a variance explanation rate of 60% or higher is generally considered acceptable. Therefore, the factor structure derived from the analysis is sufficiently valid for interpretation and further statistical analysis.

Table 7 Factor analysis

Factors	Code	Items	Factor loading
Unauthorized access and use of IT	UA1	Engaging in identity theft	0.881
	UA2	Concealing identity and deceiving co-workers	0.809
	UA3	Unauthorized access to coworkers' computers	0.8
	UA4	Concealing identity online and deceiving co-workers	0.663
Cyberslacking or cyberloafing	CS1	Browsing away work time	0.839
	CS2	Sending/receiving personal emails	0.754
	CS3	Playing computer games	0.638
	CS4	Engaging in computer rage	0.615
	CS5	Smearing the company online	0.61
Computer abuse	CA1	Encrypting company data and taking data hostage	0.809
	CA2	Spreading viruses in work on computers	0.741
	CA3	Unauthorized installation of hardware and software in company computers	0.738
	CA4	Hacking and intrusion into computer resources	0.558
	CA5	Posting critical company information online	0.522
Cyberaggression	CAG1	Sending spam and mass email messages	0.762
	CAG2	Spreading rumors and gossip about co-workers electronically	0.691
	CAG3	Distributing pornography content to co-workers	0.646
	CAG4	Distributing violent and hatred content online	0.617

Table 8. KMO and Bartlett's Test

KMO and Bartlett's Test		
Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		0.881
Bartlett's Test of Sphericity	Approx. Chi-Square	3319.600
	df	153
	Sig.	0.000

The Kaiser-Meyer-Olkin (KMO) measure and Bartlett's test are used to assess whether the dataset is suitable for factor analysis.

According to the results in the table, the KMO value is 0.881, which is considered excellent, indicating that the dataset is well-suited for factor analysis.

Bartlett's test evaluates whether the correlation matrix significantly differs from an identity matrix. The results show that the correlations are statistically significant, confirming that factor analysis is appropriate. Based on these findings, the dataset meets the requirements for factor analysis, indicating that the analysis can be conducted effectively.

International Journal of Social Science and Humanities Research-MIYR
Volume 5, Issue 2, pp.1~20, 2025
ISSN(print): 2788-9092, ISSN(Online): 2788-9106
https://youngres.com https://doi.org/10.53468/mifyr.2025.05.02.01

Table 9. Reliability Statistics

	Reliability Statistics	
	Cronbach's Alpha	N of Items
Cyberdeviance	0.862	18
Unauthorized access and use of IT	0.861	4
Cyberslacking	0.790	5
Computer abuse	0.739	5
Cyberaggression	0.646	4

The Cronbach's Alpha value for the 18-question scale was found to be 0.862, indicating a high level of reliability in measuring the overall factors of the study.

In social sciences and behavioral research, a Cronbach's Alpha ≥ 0.7 is generally considered acceptable for reliability assessment. While the Cyberaggression factor had a slightly lower Cronbach's Alpha value of 0.646, it still falls within the "acceptable" range. Overall, the measurement scale demonstrates good internal consistency, confirming that the data is suitable for further analysis.

4.4 ANOVA Test Results

Table 10. ANOVA of Cyber Deviance Dimensions Across IT Skill Levels

ANOVA - IT skill levels						
		Sum of Squares	df	Mean Square	F	Sig.
Unauthorized access and use of IT	Between Groups	1.046	3	0.349	0.347	0.791
	Within Groups	431.954	430	1.005		
	Total	433.000	433			
Cyberslacking or cyberloafing	Between Groups	2.771	3	0.924	0.923	0.430
	Within Groups	430.229	430	1.001		
	Total	433.000	433			
Computer abuse	Between Groups	6.001	3	2.000	2.015	0.111
	Within Groups	426.999	430	0.993		
	Total	433.000	433			
Cyberaggression	Between Groups	2.689	3	0.896	0.896	0.443
	Within Groups	430.311	430	1.001		
	Total	433.000	433			

From the table, no statistically significant differences were observed among the four groups of IT skill levels.

However, for the following three types of cyber deviances, the differences between groups were statistically significant ($p < 0.05$):

- Monitoring co-workers' use of computer resources (p=0.007)
- Browsing away work time (p=0.016)
- Unauthorized installation of hardware and software on company computers (p=0.031)

Table 11. ANOVA of Some Cyber Deviances Across IT Skill Levels

		N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean	
						Lower Bound	Upper Bound
CDB_ Monitoring co-workers' use of computer resources	Basic	29	1.10	0.557	0.103	0.89	1.32
	Intermediate	252	1.50	1.286	0.081	1.34	1.66
	Advanced	112	1.76	1.526	0.144	1.47	2.04
	Expert	41	2.12	1.913	0.299	1.52	2.73
	Total	434	1.60	1.403	0.067	1.47	1.73
CDB_ Browsing away work time	Basic	29	2.59	2.147	0.399	1.77	3.40
	Intermediate	252	2.19	1.737	0.109	1.98	2.41
	Advanced	112	2.80	1.921	0.182	2.44	3.16
	Expert	41	2.78	2.056	0.321	2.13	3.43
	Total	434	2.43	1.862	0.089	2.26	2.61

Levene's test for homogeneity of variances indicated that the data exhibited heterogeneous variances. Therefore, the Welch ANOVA and Games–Howell post hoc test were used, as these methods are appropriate when variance is unequal across groups.

In the basic IT skill level group, participants provided identical responses ("Never") to the question regarding **"** Unauthorized installation of hardware and software in company computers**"**, resulting in zero variance. Due to this lack of distribution, Welch ANOVA could not produce meaningful results for this variable.

According to the Multiple Comparisons (Games–Howell) test, the behavior **"**Monitoring co-workers' use of computer resources**"** showed significantly higher mean scores among the advanced and expert IT skill groups compared to the basic IT skill group. This suggests that employees with higher IT skills are more likely to monitor and take an interest in their colleagues' use of computer resources.

5. CONCLUSION AND DISCUSSION

This study examined the frequency of cyber deviances among employees in Mongolia's banking sector and assessed whether these behaviors vary based on IT skill levels. The key conclusions of the study are as follows:

All forms of cyber deviance were observed to some extent, indicating their presence in workplace environments. Among these, cyberslacking—spending time on non-work-related activities during office hours—was the most frequently reported behavior. Additionally, within the category of cyberaggression, spreading rumors and gossip online was identified as prevalent behavior.

Factor analysis confirmed the reliability of the measurement model, demonstrating that it can be used to assess cyber deviance in future studies.

No statistically significant differences were found between IT skill levels and the overall frequency of cyber deviance types. However, employees with higher IT skills were more likely to monitor co-workers' use of computer resources.

Given the presence of cyber deviances, it is important to develop preventive policies to manage and mitigate their impact.

The banking sector, as a high-trust industry with strict cybersecurity policies, has already implemented regulatory measures that may contribute to reducing cyber deviance. Therefore, it is recommended that future research analyzes and compares preventive strategies across different financial institutions.

Recommendations for the Banking Sector

To effectively prevent and manage cyber deviance in the banking sector, the following recommendations are proposed:

Implement international cybersecurity standards such as Information Security Management Systems (ISMS) to mitigate risks related to cyber deviance.

Regularly conduct training sessions and awareness programs to instill a cybersecurity-conscious culture and encourage ethical IT practices among employees.

Continuously monitor emerging trends in cyber deviance and engage employees in discussions about potential future threats and new challenges posed by technological advancements.

Refine measurement methodologies for cyber deviance and conduct periodic assessments within organizations to implement data-driven preventive measures.

Develop structured risk assessment and monitoring systems within banks to ensure ongoing evaluation of cybersecurity threats and deviant behaviors in the workplace.

Study Limitations

This study focused exclusively on Mongolia's banking sector, which may limit cross-cultural and industry-wide applicability of the findings.

The study relied on a self-reported 7-point Likert scale, which may not fully capture the actual prevalence of cyber deviance due to potential response bias.

Instead of measuring individual self-reports, the study assessed perceptions of colleagues' deviant behaviors. Since cyber deviance is often covert, some behaviors may not have been fully observed or reported.

The study only considered IT skill level as a key variable, without incorporating psychological or social factors that may influence cyber deviance.

The study was conducted at a specific point in time, limiting its ability to capture the long-term impact of technological advancements on cyber deviant behaviors.

The study relied on quantitative data, which may not provide a deep qualitative understanding of employees' motivations and reasoning behind cyber deviant behaviors.

Future Research Directions

Expanding the study to multiple industries and conducting comparative analyses could provide valuable cross-sector insights.

Incorporating qualitative research methods alongside quantitative approaches could offer a deeper understanding of the underlying motivations behind cyber deviance.

Examining psychological and social factors that influence cyber deviance could enhance the explanatory power of future research.

Considering the impact of technological advancements over time and conducting longitudinal studies would provide valuable insights into the evolution of cyber deviance.

References

[1] S. Addas, A. Pinsonneault, “E-Mail Interruptions and Individual Performance: Is There a Silver Lining?” MIS Quarterly, 42(2018): 381. doi: https://www.jstor.org/stable/26630239

[2] S. Chatterjee, S. Sarker, J. S. Valacich, “The behavioral roots of information systems security: Exploring key factors related to unethical IT use,” Journal of Management Information Systems, 31.4(2015): 49–87, doi: 10.1080/07421222.2014.1001257.

[3] K. H. Guo, Y. Yuan, N. P. Archer, C. E. Connelly, “Understanding nonmalicious security violations in the workplace: A composite behavior model,” Journal of Management Information Systems, 28. 2(2011): 203–236, doi: 10.2753/MIS0742-1222280208.

[4] M. L. Jensen, M. Dinger, R. T. Wright, J. B. Thatcher, “Training to Mitigate Phishing Attacks Using Mindfulness Techniques,” Journal of Management Information Systems, 34.2(2017): 597–626, doi: 10.1080/07421222.2017.1334499.

[5] S. Tams, J. B. Thatcher, V. Grover, “Concentration, competence, confidence, and capture: An experimental study of age, interruption-based technostress, and task performance,” J Assoc Inf Syst, 19.9(2018): 857–908, doi: 10.17705/1jais.00511.

[6] D. P. Ford, A. Hancock, “A Review and Extension of Cyber-Deviance Literature: Why It Likely Persists,” 2018. [Online]. Available: https://www.researchgate.net/publication/323755999

[7] S. Kiesler, “The hidden messages in computer networks,” 1986.

[8] S. Venkatraman, C. M. K. Cheung, Z. W. Y. Lee, F. D. Davis, V. Venkatesh, "The 'Darth' Side of Technology Use: An Inductively Derived Typology of Cyberdeviance," Journal of Management Information Systems, 35.4(2018): 1060–1091, doi: 10.1080/07421222.2018.1523531.

[9] D. Fontein, "How to write a social media policy for your company," Hootsuite, Feb. 2017.

[10] A. Malik, S. Sinha, S. Goel, "A Qualitative Review of 18 Years of Research on Workplace Deviance: New Vectors and Future Research Directions," Hum Perform, 2021, doi: 10.1080/08959285.2021.1948548.

[11] Y. Chen, X. Wang, J. Benitez, X. Luo, D. Li, "Does Techno-invasion Lead to Employees' Deviant Behaviors?" Journal of Management Information Systems, 39.2(2022): 454–482, doi: 10.1080/07421222.2022.2063557.

[12] V. Venkatesh, C. M. K. Cheung, F. D. Davis, Z. W. Y. Lee, "Cyberslacking in the workplace: Antecedents and effects on job performance," MIS Q, 47.1(2023): 281–316, doi: 10.25300/MISQ/2022/14985.

[13] T. Weatherbee, E. K. Kelloway, "A case of cyberdeviancy: Cyberaggression in the workplace," in Handbook of Workplace Violence, SAGE Publications Inc., 2006, pp. 445–488. doi: 10.4135/9781412976947.n19.

[14] J. Magnusson, F. Carlsson, M. Matteby, P. Ndanu Kisembo, and D. Brazauskaite, "The polyphony of deviance: the impact of deviant workplace behavior on digital transformation," Transforming Government: People, Process and Policy, Jan. 2024, doi: 10.1108/TG-09-2023-0144.

[15] T. Weatherbee, "Counterproductive use of technology at work: Information & communications technologies and cyberdeviancy," Human Resource Management Review, 20.1(2010): 35–44, doi: 10.1016/j.hrmr.2009.03.012.

[16] S. Venkatraman, C. M. K. Cheung, Z. W. Y. Lee, F. D. Davis, V. Venkatesh, "The 'Darth' Side of Technology Use: An Inductively Derived Typology of Cyberdeviance," Journal of Management Information Systems, 35.4(2018):1060–1091, doi: 10.1080/07421222.2018.1523531.

[17] F. Mohd Shamsudin, C. Subramaniam, A. Said Alshuaibi, "The Effect of HR Practices, Leadership Style on Cyberdeviance: The Mediating Role of Organizational Commitment," 2012.

[18] Z. Zhao, "The Causes and Measures of Online Deviance," 2023.

[19] D. H. Doty, W. H. Glick, "Typologies As a Unique Form Of Theory Building Toward Improved Understanding and Modeling," 1994.

AUTHOR'S INTRODUCTION

1. First Author

Narantungalag Ganbat narantungalag.g@ufe.edu.mn

Doctoral student at the Graduate School of University of Finance and Economics, Ulaanbaatar, Mongolia

Work: Senior lecturer, Business management department, University of Finance and Economics, Ulaanbaatar, Mongolia

Work field: Education, Business management

2. Corresponding-Authors

Gerelmaa Damba gerelmaa.d@ufe.edu.mn

2003- Ph.D in Management, Academy of Management, Mongolia

Work: Professor, Business management department, University of Finance and Economics, Ulaanbaatar, Mongolia

Work field: Education, Management and governance

3. Co-Authors

Nandin-Erdene Banzragch nandinerdene.b@ufe.edu.mn

2012- Master in Marketing, Australian National University, Australia

Work: Senior lecturer, Marketing management department, University of Finance and Economics, Ulaanbaatar, Mongolia

Work field: Education, Marketing management

4. Co-Authors

Delgersaikhan Bold delgersaikhan.b@ufe.edu.mn

2011- MAFM, DeVry university, USA

Work: Senior lecturer, Accounting department, University of Finance and Economics

Work field: Education, Managerial accounting

5. Co-Authors

Tamir Enkhbat tamir.en@ufe.edu.mn

2023- MBA, University of Finance and Economics, Ulaanbaatar, Mongolia

Work: Lecturer, Business management department, University of Finance and Economics, Ulaanbaatar, Mongolia

Work field: Education, Human resource management