Open Access

Public Organization Management

Vol. 14(2), (Series 54): 109-132/ 2026

https://doi.org/10.30473/ipom.2026.74401.5178

E-ISSN: 2538-600X P-ISSN: 2322-522X

ORIGINAL ARTICLE

Providing a Comprehensive Model to Control and Reduce Cyberloafing in Organizations

Rahmatollah Gholipor [1], Seyed kamal Vaezi [2], Maysam Karimi[3*]

1. Professor, Department of Business Strategy and Policy, Faculty of Business Management, College of Management, University of Tehran, Tehran, Iran.
2. Associate Professor., Department of Leadership and Human Capital, Faculty of Public Administration and Organizational Sciences, College of Management, University of Tehran, Tehran, Iran.
3. MSc. Student, Department of Public Policy and Public Administration, College of Management, University of Tehran, Tehran, Iran.

*Correspondence
Maysam Karimi
E-mail: maysamkarimi@ut.ac.ir

Receive Date: 24/April/2025
Revise Date: 03/July/2025
Accept Date: 23/July/2025

How to cite
Gholipor, R., Vaezi, S.K., & Karimi, M (2026). Providing a Comprehensive Model to Control and Reduce Cyberloafing in Organizations. *Public Organization Management*, 14(2), 109-132

EXTENDED A B S T R A C T

Introduction

Cyberloafing-employees' use of internet-enabled devices for personal, non-work activities during paid working time-has become a pervasive issue in modern organizations. Although digital technologies facilitate communication and service delivery, they also enable off-task behaviors that may reduce productivity, disrupt workflows, and increase security risks. These concerns are particularly salient in public-sector organizations, where accountability, service continuity, and information integrity are critical to public value creation. In Iran, public organizations operate within a distinct socio-cultural and institutional context characterized by hierarchical governance structures, strong regulatory oversight, and uneven technological infrastructure. Such conditions shape both the antecedents of cyberloafing and the acceptability of managerial responses. Consequently, findings from private-sector or Western contexts cannot be directly generalized without contextual adaptation. This study aims to develop a context-sensitive model of cyberloafing in Iranian public organizations by identifying its key antecedents, feasible control mechanisms, and culturally appropriate preventive and mitigative strategies. Specifically, the research addresses three questions: (1) which individual, organizational, and technological factors contribute to cyberloafing; (2) which control mechanisms are perceived as effective, feasible, and ethically acceptable; and (3) which strategies can reduce cyberloafing while respecting employee privacy and organizational norms. By integrating behavioral and socio-technical perspectives, the study contributes both theoretical insight and practical guidance for public-sector managers and policymakers.

Methodology

This study adopted a qualitative, exploratory design using reflexive thematic analysis. Participants were selected through purposeful and snowball sampling and included managers, HR professionals, organizational development experts, and applied psychologists working in

Iranian public-sector institutions. In total, twenty-one semi-structured interviews were conducted with professionals affiliated with governmental organizations, public universities, and quasi-public bodies. Interviews explored three domains: patterns of off-task online behavior, existing control practices and policies, and recommended preventive or mitigative strategies aligned with local norms. Interviews lasted 45-75 minutes, were audio-recorded with informed consent, and transcribed verbatim. Data analysis followed the three-stage approach proposed by King and Horrocks. First, open coding was used to capture descriptive accounts. Second, related codes were clustered through axial coding to develop interpretive categories. Finally, higher-order themes were constructed to generate a coherent conceptual model encompassing antecedents, control mechanisms, and preventive strategies. Trustworthiness was enhanced through peer debriefing, member checking, reflexive memo-writing, and maintenance of an audit trail. Ethical principles-including confidentiality, anonymization, and voluntary participation-were strictly observed.

Findings

The analysis yielded three interrelated themes: antecedents of cyberloafing, control mechanisms and implementation challenges, and preventive and mitigative strategies. Antecedents of cyberloafing emerged from the interaction of individual, organizational, and technological factors. At the individual level, low intrinsic motivation, burnout, weak self-regulation, and generational digital habits encouraged short online "micro-breaks." Organizational contributors included unclear job expectations, weak performance feedback, misaligned reward systems, and cultural tolerance of minor rule violations. Technological antecedents involved ubiquitous internet access, poor separation between work and personal use, and inefficient work systems that increased susceptibility to digital distractions. Control mechanisms and challenges ranged from restrictive technical measures (e.g., filtering and monitoring) to supportive tools (e.g., productivity dashboards and self-monitoring notifications). While restrictive approaches were seen as effective in the short term, they were widely criticized for undermining trust and provoking resistance. Key implementation challenges included privacy concerns, inaccurate monitoring data, administrative burden, and inconsistent enforcement. Preventive and mitigative strategies emphasized motivational and participatory approaches. Participants favored job redesign, transparent reward systems, digital literacy and stress-management training, and participatory policy development. Non-intrusive monitoring and aggregated feedback mechanisms were viewed as more acceptable and effective than punitive surveillance.

Discussion and Conclusion

This study demonstrates that cyberloafing in Iranian public organizations is a socio-technical phenomenon shaped by individual motivations, organizational structures, and digital affordances. Approaches relying solely on surveillance and restriction risk eroding trust and may generate counterproductive behaviors. In contrast, strategies that combine participatory governance, motivational job design, and responsible technology use appear more sustainable. The findings support an integrative framework linking behavioral factors—such as motivation and self-regulation—with systems-level elements including leadership

practices, job design, and IT infrastructure. Practically, the study proposes a phased approach involving diagnostic assessment, co-designed internet usage policies, pilot implementation of non-intrusive monitoring tools, and complementary interventions such as training and reward realignment. While limited by its qualitative design and contextual scope, this research provides a grounded foundation for future mixed-method and intervention-based studies. Overall, effective cyberloafing management in the public sector requires balanced, ethical, and context-sensitive strategies that protect both organizational performance and employee well-being.

K E Y W O R D S
Cyberloafing, Public Organizations, Theme Analysis , Productivity, Strategy.