

הפרת ביטחון מידע בקבוצות וואטסאפ ארגוניות (פוסטר)

נעמה איזנרייך	אבי ברששת	חגית מישר-טל
מכון טכנולוגי חולון	מכון טכנולוגי חולון	מכון טכנולוגי חולון
naama235@gmail.com	avibar6t@gmail.com	hagitm@gmail.com

Information Security Violations in Organizational WhatsApp Groups (Poster)

Naama Eisenreich	Avi Barsheshet	Hagit Meishar-Tal
Holon Institute of Technology (HIT)	Holon Institute of Technology (HIT)	Holon Institute of Technology (HIT)

Abstract

Recently WhatsApp application has become a hit among smartphone users in Israel. The network enables the opening of discussion groups and information sharing between the users of Smartphones easily. In Many organizations workers' WhatsApp groups are opened and used for sharing work-related information.

Using WhatsApp in organizations increases the potential of violations of information security policies and creates ethical dilemmas regarding the rules of sharing information among employees in the organization.

This study tries to measure the amount of information security violations in security-oriented organizations' WhatsApp groups, and to examine which factors are related to the information security violations. This would establish an empirical foundation for organizational improvement of information security obedience.

Surveys that were answered by 63 employees of two security-oriented organizations were analyzed, and three conclusions were deduced: First, information security is related to organizational social climate. Therefore, information security obedience behavior should be enforced on both employees and management. Second, managers' behavior must be monitored, since their WhatsApp activity is related to employees' behavior and since they perceive information security violation as relatively high. Last is the fear of punishment, which is one of the main factors that relate to Information security violations.

Keywords: WhatsApp, information security, organizational culture.

תקציר

לאחרונה הפכה רשת הוואטסאפ ללהיט בקרב משתמשי סמארטפונים בישראל. הרשת מאפשרת פתיחת קבוצות לדיון ושיתוף מידע בין בעלי סמארטפונים בקלות רבה. בארגונים רבים נפתחות קבוצות וואטסאפ של עובדים הקשורות לעבודה. בארגונים רבים, ובייחוד בארגונים בטחוניים, חשיפת מידע ארגוני מסווג על ידי גורמים מתוך המערכת מהווה סיכון ארגוני חמור (Chen & Li, 2014, p. 1). מדיניות ארגונית בנושא לא תמיד מיושמת מצד העובדים (Pahnilaa, Siponen & Mahmood, 2007). השימוש בוואטסאפ בארגונים מהווה

נקודת תורפה המזמנת הפרות של מדיניות ביטחון מידע ויוצר דילמות אתיות באשר לכללי שיתוף המידע בין העובדים בארגון.

המחקר מנסה לברר עד כמה נפוצה התופעה של הפרת ביטחון מידע בוואטסאפ ואילו גורמים קשורים להפצת המידע מסווג על ידי עובדים בארגונים ביטחוניים. מטרת המחקר היא להניח יסוד אמפירי שיאפשר לארגונים לגבש תכנית פעולה ולהטמיע שינוי ארגוני וכללי התנהגות נאותים בתחום ביטחון המידע בעולם של שיתופיות מקוונת.

שאלון הופץ בקרב 63 עובדים של שני ארגונים בעלי אוריינטציה בטחונית. הנשאלים התבקשו לתאר את הרגלי השימוש שלהם בוואטסאפ בהקשר להפרת ביטחון המידע בוואטסאפ ולאקלים הארגוני והמוסכמות החברתיות בארגון שבו הם עובדים.

הממצאים מצביעים על קשר בין מידת הפעילות הפרטית בוואטסאפ לבין מידת הפעילות בוואטסאפ בנושאי עבודה, דבר התומך בפרשנות לתיאוריית העולמות הקטנים של ברנט, גיגר ותומפסון (Burnett, Jaeger, & Thompson, 2008). נמצא קשר מובהק בין מידת ההפרה הארגונית, לבין מידת הפעילות של הקולגות ($r = .326, p < 0.01$) והמנהלים ($r = .432, p < 0.01$) בוואטסאפ בנושאי עבודה. זהו חיזוק נוסף לכך שהשפעה חברתית מצד ההנהלה הבכירה, המנהלים והקולגות קשורה למידת היישום של מדיניות אבטחת המידע (Pahnilaa et al., 2007). נמצא קשר מובהק בין מידת ההפרה הארגונית לבין החשש להיענש ($r = .316, p < 0.05$) ולהיתפס ($r = .300, p < 0.05$). הדבר מחזק את התיאוריה של הרתי וראו (Herath & Rao 2009), לפיה לחשש להיתפס יש השפעה על כוונתם של עובדים לציית למדיניות ביטחון המידע. מידת ההפרה הארגונית הגבוהה ביותר דווחה על ידי המנהלים הזוטרים, והנמוכה ביותר על ידי עובדים שאינם מנהלים. ההנחה הייתה כי ימצא הבדל בממוצעי הדיווחים של קבוצות אלה על גורמים הקשורים להפרה הארגונית, אולם לא עלו ממצאים מובהקים. בין שני הארגונים קיים הבדל מובהק ($t(61) = 2.34, p < 0.05$) בממוצע הדיווחים על מידת ההפרה הארגונית. ההנחה הייתה שגורמים אשר נמצאו קשורים למידת ההפרה הארגונית יהיו קשורים להבדל בין הארגונים אולם לא עלו ממצאים מובהקים.

שלוש מסקנות עיקריות עולות מניתוח הממצאים: ראשית, הפרת ביטחון המידע קשורה לאקלים החברתי, לכן יש להקפיד על מדיניות אבטחת המידע בארגון בקרב העובדים והמנהלים כאחד. שנית, יש להקפיד על התנהלות המנהלים, זאת לאור הקשר בין פעילותם בוואטסאפ לבין הפרת ביטחון המידע על ידי העובדים וגם בגלל הדיווח על הפרה ארגונית שהיה גבוה במיוחד בקרבם. לבסוף, החשש מענישה עולה כאחד הגורמים שקשורים להפרת ביטחון המידע. כדאי להגדיר במדיניות הארגון פעולות ענישה מידתיות ומרתיעות, להביא לידיעת העובדים ולמשן בעת הצורך.

מילות מפתח: וואטסאפ, ביטחון מידע, תרבות ארגונית, אתיקה ארגונית.

מקורות

- Burnett, G., Jaeger, P.T., & Thompson, K.M. (2008). Normative behavior and information: The social aspects of information access. *Library & Information Science Research*, 30, 56-66.
- Chen, H. & Li, W. (2014). Understanding organization employee's information security omission behavior: an integrated model of social norm and deterrence. *Proceeding of the 19th Pacific Asia Conference on Information Systems*. Retrieved from <http://www.pacis-net.org/file/2014/1943.pdf>
- Herath, T. & Rao, H.R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, 47, 154-165.
- Pahnilaa, S., Siponen, M. & Mahmood, A. (2007). Employees' Behavior towards IS Security Policy Compliance. *Proceedings of the 40th Hawaii International Conference on System Sciences*. Retrieved from: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.106.7038&rep=rep1&type=pdf>