Society Culture Media

Vol 14. Spring 2025

Research Paper

Crisis Communication Strategies in Compaines' Image Repair:A Comparative Study of Tapsi and Snappfood's Performance in Facing Their Information Systems Hacking

Reihaneh Razmara[1] , Farzad Gholami[2]

Received: May.11,2025, Accepeted:Jun. 4,2023

DOI: 10.22034/scm.2025.522866.1873

Abstract

This research examines how Iranian online services use crisis response strategies, focusing on image repair strategies during the hacking crisis of these services. Using William Benoit's image repair theory, the media messages of these companies—including Tapsi and Snappfood's X tweets, Tapsi and Snappfood's Instagram posts, announcements and content published on Snapp and Tapsi websites, hacker group announcements on Telegram, and user comments on X—were studied. For data analysis, the theory-driven content analysis method was used. The results indicate that the "reducing offensiveness of event" strategy (transcendence type) and the "corrective Action" strategy were used by both companies. Tapsi used denial, evasion of responsibility, reducing offensiveness of event, corrective action, and mortification; while Snapp used reducing offensiveness of event and corrective action. The strategies were incompletely implemented by both companies, and both hacking incidents faced negative user reactions on social media. Given the monopoly position of these companies in service provision and the absence of a competitive environment, they have undertaken minimal efforts to mitigate crisis damages to stakeholders and preserve their image.

Keywords: Image repair, crisis communication, hack, Snappfood, Tapsi

[1] . Master's student in Social Communication Sciences, Faculty of Social Sciences, University of Tehran, razmara.reihaneh@ut.ac.ir

[2] . Assistant Professor, Department of Social Communication Sciences, Faculty of Social Sciences, University of Tehran, (Corresponding Author), Farzadgholami@ut.ac.ir

Introduction

Nowadays, information and security crises have become an inevitable part of the challenges faced by large organizations and corporations. Data hacking is a major security crisis that leads to widespread violations of user privacy. Hackers target large organizations with motives such as extortion, data trafficking, or gaining notoriety. Companies, in turn, employ various strategies for crisis communication and corrective measures in response to such breaches. These crises not only raise widespread concerns about data security and user privacy but can also severely damage a company's reputation and credibility. Consequently, stakeholders may lose trust in the affected companies, ultimately leading to a significant decline in profits and revenue.

Therefore, effective crisis management and the implementation of crisis communication strategies are crucial for businesses. In this context, image repair strategies play a vital role in restoring public trust. Thus, the focus of this research is to examine how two companies, Snappfood and Tapsi, utilized crisis communication strategies following the hacking of their information systems to mitigate the damage caused by the crisis and preserve their corporate image among users. Subsequently, we will briefly outline the crises these two companies faced.

Since corporate Image is a critical concern, companies in crisis situations not only strive to mitigate the damage but also employ Image repair strategies to design their post-crisis messaging, thereby safeguarding their image and credibility. In this study, using thematic analysis and an examination of Snappfood and Tapsi's media responses following the crisis, we aim to demonstrate how these companies applied Benoit's Image repair strategies to minimize harm and rebuild their Image among customers. Accordingly, this research seeks to answer the following three questions:

1. Which of Benoit's reputation repair strategies were used in Snappfood and Tapsi's post-crisis media communications following the hacking of their systems?
2. How do the strategies employed by Tapsi and Snappfood differ from each other?
3. How did users react to these crises?

Purpose

A review of crisis communication research indicates that hacking of organizational information systems is one of the most severe crises faced by organizations in the internet age. However, within the Iranian academic sphere, no study has yet been published that examines information system hacking from a crisis communication perspective—particularly through the lens of image repair theory.

Thus, this study can serve as a starting point for exploring crisis response strategies, specifically the application of image repair theory, to guide organizations in managing such critical situations.

Methodology

In this study, we employed theory-driven content analysis, a widely-used method for analyzing media texts. We specifically focused on Benoit's theoretical framework to guide our content analysis.

We examined a comprehensive dataset to investigate the crisis communication strategies of both companies, including:

1 .X (Twitter) posts by Tapsi and Snappfood 2. Instagram posts by Tapsi, Snapp, and Snappfood

3 .Official statements published on Tapsi and Snappfood websites 4 .Announcements in the hacker group's Telegram channel 5 .User tweets responding to Tapsi and Snappfood's reactions.

We collected all tweets, Instagram posts, and website content from:

-The hacking date (September 2, 2023 for Tapsi; December 31, 2023 for Snappfood)

-Until the article's writing date (March 5, 2025)

-For Tapsi: The Twitter thread by Milad Monshipour (Tapsi's founder) served as the primary reference

-For Snappfood: The official Snappfood Twitter account and the company's 2023 annual report were analyzed

(Note: While we examined all tweets from both accounts during the post-hack period, none of them addressed the hacking incident on their Instagram accounts.)

Researchers conducted thematic analysis to identify crisis communication strategies based on the theoretical framework. To assess user reactions (our secondary research question), we performed data-driven content analysis of:

131- relevant user responses to Monshipour's tweet (after removing irrelevant ones)

-157 relevant responses to Snappfood's tweet

(Note: User reactions on Instagram weren't analyzed as the companies didn't post about the hacking incident there.)

We also analyzed 10 announcements from the hacker group (IRL eaks Telegram channel) to enhance the findings' accuracy.

Findings

The table below compares the image repair strategies employed by Tapsi and Snappfood following the hacking of their information systems:

Table 1: Comparison of Snap Food and Tapsy's responses to the hacking of their information systems

Strategy	Type	Platform
Denial	Shift the Blame	TAPSI
Evasion of Responsibility	Good Intentions	TAPSI
Reducing Offensiveness of Event	Bolstering	Snappfood
	Minimization	Snappfood
	Transcendence	TAPSI- Snappfood
	Attack Accuser	Snappfood
Corrective Action	-	TAPSI- Snappfood
Motification	-	TAPSI

As clearly demonstrated in the table above, Tapsi implemented a comprehensive array of image repair strategies following the data breach, including: denial (shift the blame), evasion of responsibility (good intentions), reducing offensiveness (transcendence), corrective action, and mortification. In contrast, Snappfood adopted a more limited approach, utilizing only two primary strategies: reducing offensiveness (through bolstering, minimization, transcendence, and attack accuser tactics) along with corrective action strategies. This strategic divergence highlights fundamentally different approaches to reputation management in crisis situations, with Tapsi employing a more diversified response framework while Snappfood focused on minimizing perceived damage through selective techniques.

User Reactions Analysis:

On Instagram, users who became aware of the hacking incident posted comments related to the breach under the companies' unrelated posts (those addressing other topics). While the number of such comments remained limited, none received responses from the social media administrators of either service.

The response pattern on X (formerly Twitter) proved markedly different. Notably, the Snappfood hack became a trending topic on Persian X, generating substantial user engagement. Since the hacking group had leaked samples of the compromised data, many tweets featured users humorously engaging with and mocking the leaked samples.

Conclusion

Overall, the analysis reveals that both companies employed similarly ineffective approaches, failing to fully manage the crisis. While the situation was eventually contained, this was likely due more to user apathy—where many customers showed little concern for their compromised data, defaulted to humor as their primary reaction, and had no competitive alternatives to Tapsi and Snappfood—rather than effective crisis management.

The companies' flawed strategies, particularly delayed communication and denial (evidenced by their silence on Instagram), exacerbated negative user reactions, at least in the digital sphere. Although some corrective measures and cybersecurity improvements were implemented, the initial denial and lack of transparency significantly undermined their crisis response.

This case underscores the urgent need for companies to reform their crisis communication strategies, particularly when handling such incidents. Crucially, organizations must prioritize culturally and socially attuned crisis communication tailored to Iran's context to rebuild customer trust.

Proactively investing in robust crisis communication frameworks should be viewed as forward-looking strategic expenditure. Such investment not only safeguards reputation and stakeholder interests during crises but also mitigates long-term financial and operational risks.

Bibliography

Allison, R., Pegoraro, A., Frederick, E., & Thompson, A. J. (2020). When women athletes transgress: An exploratory study of image repair and social media response. Sport in Society, 23(6), 1023–1041. https://doi.org/10.1080/17430437.2019.1580266

Amoroso, D. L., & Chen, Y. A. N. (2017). Constructs Affecting Continuance intention in consumers with mobile financial apps: a dual factor approach. *Journal of Information Technology Management*, *28*(3), 1-24. http://jitm.ubalt.edu/XXVIII-3/article1.pdf

Benoit, W. L. (1997). Image repair discourse and crisis communication. Public Relations Review, 23(2), 177–186. https://doi.org/10.1016/ S0363-8111(97)90023-0 https://doi.org/10.1016/S0363-8111(97)90023-0

Benoit, W. L. (2015). Accounts, Excuses, and Apologies: Image Repair Theory and Research. United States: State University of New York Press.

https://books.google.com/books/about/Accounts_Excuses_and_Apologies_Second_Ed.html?id=t1TVBAAAQBAJ

Bentley JM, Oostman KR, Shah SFA. (2018). We're Sorry But It's Not Our Fault: Organizational Apologies in Ambiguous Crisis Situations. Journal of Contingencies and Crisis Management 26(1): 138–149. https://doi.org/10.1111/1468-5973.12169

Bryant, J., Hopton, B., & Azodo, L. (2023). *Crisis communication planning: Strategies for non-governmental organizations* (S. Abdi, Trans.). Tehran: Public Relations Agents Publishing. (Original work published 2023). (in Persian)

Cheng, Y., & Cameron, G. (2018). The status of social-mediated crisis communication (SMCC) research: An analysis of published articles in 2002-2014. In L. Austin & Y. Jin (eds.), Social Media and Crisis Communication (pp. 9–20). Routledge. http://dx.doi.org/10.4324/9781315749068-2

Chiu, C. M., Chang, C. C., Cheng, H. L., & Fang, Y. H. (2009). Determinants of customer repurchase intention in online shopping. *Online Information Review*, *33*(4), 761-784. https://doi.org/10.1108/14684520910985710

Chon, M. G., & Kim, S. (2022). Dealing with the COVID-19 crisis: Theoretical application of social media analytics in government crisis management. Public Relations Review, 48(3), 102201. https://doi.org/10.1016/j.pubrev.2022.102201

Coombs, W. T. (2004). Impact of past crises on current crisis communication: Insights from situational crisis communication theory. Journal of Business Communication, 41(3), 265–289. https://doi.org/10.1177/0021943604265607

Coombs, W. T., Sherry J. Holladay. (2010). The Handbook of Crisis Communication (Handbooks in Communication and Media. Wiley-Blackwell. https://doi.org/10.1002/9781444314885

Crandall, W. R., Parnell, J. A., & Spillan, J. E. (2017). *Crisis management: Modern strategies for building management teams before and after crises* (O. Tashtazar, Trans.). Tehran: Geraresh-e Tazeh Publishing. (Original work published 2017) (in Persian). https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449

Frandsen, F., Johansen, W. (2016). Organizational Crisis Communication: A Multivocal Approach. United Kingdom: SAGE Publications. https://www.researchgate.net/publication/305943066_Organizational_Crisis_Communiication_A_Multivocal_Approach

Gholami, F., & Taghizadeh, M. (2022). *Crisis communication and local media: Framing news coverage of the 2021 floods in Kerman provincial television*

network. Journal of Society, Culture and Media, 11 (43), 11-41. (in Persian) https://www.jscm.ir/article_158627.html

Gilpin, D. R., & Murphy, P. J. (2008). *Crisis management in a complex world*. Oxford University Press. https://academic.oup.com/book/10743

Howard, J. M. (2020). Trains, Twitter and the social licence to operate: An analysis of Twitter use by train operating companies in the United Kingdom. Case Studies on Transport Policy, 8(3), 812–821. http://dx.doi.org/10.1016/j.cstp.2020.06.002

Kamboh, S. A., Ittefaq, M., & Jin, Y. (2024). Crisis communication for public organizations: Examining Pakistan Railways' use of information technology and social media for image repair. *Journal of Contingencies and Crisis Management*, 32, e12496. https://doi.org/10.1111/1468-5973.12496

Knight, Richard & Nurse, Jason R. C. (2020). A framework for effective corporate communication after cyber security incidents. Computers & Security ،99 ، 102036.. https://doi.org/https://doi.org/10.1016/j.cose.2020.102036

Kuipers, Sanneke & Schonheit, Michael. (2021). Data Breaches and Effective Crisis Communication: A Comparative Analysis of Corporate Reputational Crises. Corporate Reputation Review. http://dx.doi.org/10.1057/s41299-021-00121-9

L. Heath, Robert & O'Hair, H. Dan. (2010) Handbook of Risk and Crisis Communication. United Kingdom: Taylor & Francis.

Marzouqi, Z. (2023). *Where is the Achilles' heel of big data hacking?* Farheekhtegan, https://doi.org/10.4324/9781003070726

Monshipour, M. [@MMonshipour]. (2023, September 2). *[Tweet content in Persian]*. Twitter. Retrieved from <URL> https://x.com/MMonshipour/status/1697967020896137515?t=YxJ7ygyNeJzMlDP1iUkWYA&s=19<

Ojagh, Seyedeh Zahra (2022). Identifying crisis response strategies during the Covid-19 pandemic in the sphere of Iranian Media. Media Management Review, 1(4), 399-417. (in Persian) doi: https://doi.org/10.22059/MMR.2023.355032.1040

Olaniran, Bolanle & Potter, Andrew & Ross, Katy & Johnson, Brad. (2014). A Gamer's Nightmare: An Analysis of the Sony PlayStation Hacking Crisis. Journal of Risk Analysis and Crisis Response. 4. 151. 10.2991/jrarc.2014.4.3.4 . https://doi.org/10.2991/jrarc.2014.4.3.4

Park, Hanna. 2017. Exploring Effective Crisis Response Strategies. Public Relations Review. https://doi.org/10.1016/j.pubrev.2016.12.001.

Ruohonen, J., Hjerppe, K., & Kortesuo, K. (2024). Crisis Communication in the Face of Data Breaches. *arXiv preprint arXiv:2406.01744*. https://doi.org/10.48550/arXiv.2406.01744

Sellnow, T.L. & Seeger, M.W. (2013). Theorizing Crisis Communication. Wiley. https://books.google.com/books/about/Theorizing_Crisis_Communication.html?id=YGUQEAAAQBAJ

Spradley, R. Tyler. (2017). Crisis Communication in Organizations. In The International Encyclopedia of Organizational Communication. https://doi.org/10.1002/9781118955567.wbieoc050

Upadhyay, S., & Upadhyay, N. (2023). Mapping crisis communication in the communication research: what we know and what we don't know. *Humanities and Social Sciences Communications*, *10*(1), 1-19

Vaziri, A. (2023). *Snappfood was hacked!* [Article]. https://controladad.com/blog/khbr/snapp-food-hack

Webna. (2023). *LifeWeb analysis of user behavior: Snappfood was hacked, users tweeted and even laughed.* [Online news article]. Retrieved from <URL>https://webna.ir/39374/

Zhang, J., & Benoit, W. L. (2004). Message strategies of Saudi Arabia's image restoration campaign after 9/11. Public Relations Review, 30(2), 161–167. https://doi.org/10.1016/J.PUBREV.2004.02.006

سال چهاردهم/ بهار ۱۴۰۴

مقاله پژوهشی

استراتژی‌های ارتباطات بحران در ترمیم وجهه شرکت‌ها: مطالعه مقایسه‌ای عملکرد تپسی و اسنپ‌فود در مواجهه با هک سامانه های اطلاعاتی آنها

• ریحانه رزم آرا[۱]، فرزاد غلامی[۲]

تاریخ دریافت:۰۴/۲/۲۱، تاریخ تایید:۰۴/۳/۱۴

DOI: 10.22034/scm.2025.522866.1873

چکیده:

این پژوهش به بررسی نحوه استفاده سرویس‌های آنلاین ایرانی از استراتژی‌های پاسخ به بحران با تمرکز بر استراتژی‌های ترمیم وجهه در بحران هک این سرویس‌ها می‌پردازد. با استفاده از نظریه ترمیم وجهه ویلیام بنت پیام‌های رسانه‌ای این شرکت‌ها شامل توییت‌های ایکس تپسی و اسنپ‌فود، پست‌های اینستاگرامی تپسی و اسنپ‌فود، اطلاعیه‌ها و محتوای منتشر شده در سایت اسنپ و تپسی، اطلاعیه های گروه هکری در تلگرام و نظرات کاربران در ایکس مورد مطالعه قرار گرفتند . برای تحلیل داده‌ها از روش تحلیل محتوای نظریه‌محور استفاده شده است. نتایج پژوهش بیانگر آن است که استراتژی کاهش آسیب از نوع تعالی و استراتژی اقدام تصحیحی توسط هر دو شرکت مورد استفاده قرار گرفته است. تپسی از انکار، طفره رفتن از مسئولیت ، کاهش آسیب، اقدام تصحیحی و تاسف و اسنپ از کاهش آسیب و اقدام تصحیحی استفاده کرده است.. استراتژی‌ها توسط هر دو شرکت به صورت ناقص استفاده شده اند و هر دو هک در رسانه‌های اجتماعی با واکنش منفی کاربران مواجه بوده است. می‌توان گفت انحصار ارائه خدمات توسط این شرکت‌ها و نبود فضای رقابتی باعث شده است که این شرکت‌ها حداقل اقدامات برای کاهش آسیب‌های بحران به ذی نفعان و تلاش برای حفظ وجهه را داشته باشند.

واژگان کلیدی: ترمیم وجهه، ارتباطات بحران، هک، اسنپ‌فود، تپسی

---

[۱]. دانشجوی کارشناسی ارشد علوم ارتباطات اجتماعی دانشکده علوم اجتماعی دانشگاه تهران، razmara.reihaneh@ut.ac.ir

[۲]. استادیار گروه علوم ارتباطات اجتماعی دانشکده علوم اجتماعی دانشگاه تهران، نویسنده مسئول، Farzadgholami@ut.ac.ir

مقدمه

یکی از ابعاد مدیریت بحران، «ارتباطات بحران» است که نه به‌عنوان حلال بحران بلکه برای برقراری ارتباط مؤثر با ذی‌نفعان به کار می‌رود (غلامی و تقی‌زاده، ۱۴۰۱: ۱۶). بر مبنای آنچه که موری و شوهن (۱۹۹۲) بیان کرده‌اند به لحاظ زمانی ریشه ارتباطات بحران را می‌توان به عملکرد بسیار موفقیت‌آمیز شرکت جانسون و جانسون در ماجرای مسمویت و مرگ چند نفر با کپسول های تلنول[1] این شرکت مرتبط دانست، به عبارتی عملکرد این شرکت در بازیابی سهمش از بازار و حفظ وجهه خود پس از این به بحران به حدی اثرگذار بود که محققان را به این فکر واداشت که با فرآیند «مهندسی معکوس» چگونگی مدیریت بحران و به طور خاص ارتباطات بحران این شرکت را به مدلی تبدیل کنند، که بتوان از آن در موقعیت‌های دیگر بهره‌برداری کرد (گیلیپین و مورفی، ۲۰۰۸: ۱۷). بنابراین می‌توان گفت که ارتباطات بحران یک حوزه مطالعاتی چندرشته‌ای است که شامل مجموعه‌ای از اقداماتی می‌شود که سازمان‌ها از طریق آنها قبل، در حین و پس از بحران‌ها ارتباط برقرار می‌کنند تا سطحی از عملکرد عادی خود را حفظ کنند (Spradley, 2017).

در یک تعریف کلی ارتباطات بحران را می‌توان به طور گسترده به‌عنوان جمع‌آوری، پردازش و انتشار اطلاعات مورد نیاز برای رسیدگی به یک وضعیت بحرانی تعریف کرد. به این صورت که در مرحله پیش از بحران، ارتباطات بحران حول محور جمع‌آوری اطلاعات درباره خطرات بحران، تصمیم‌گیری در مورد نحوه مدیریت بحران‌های احتمالی، و آموزش افرادی که در فرآیند مدیریت بحران نقش خواهند داشت، می‌چرخد. این آموزش شامل اعضای تیم بحران، سخنگویان بحران و هر فردی که در پاسخ به بحران کمک خواهد کرد، می‌شود. در حین بحران ارتباطات بحران شامل جمع‌آوری و پردازش اطلاعات برای تصمیم‌گیری تیم بحران، همراه با ایجاد و انتشار پیام‌های بحرانی برای افراد خارج از تیم مانند ذی‌نفعان (تعریف سنتی ارتباطات بحران) است. پس از بحران نیز، این فرآیند به بررسی تلاش‌های مدیریت بحران، منتقل کردن تغییرات لازم به افراد، و ارائه پیام‌های پیگیری بحران در صورت نیاز می‌پردازد(Coombs, 2010, p20. ارتباطات بحران دارای اصولی است که می توان آن را برای بحران‌های با منشا مختلف به کار گرفت، به این معنا که می‌توان از پتانسیل‌ها و ظرفیت‌های ارتباطی و رسانه‌ای

---

[1] .Tylenol

برای مدیریت بحران‌های مختلف فارغ از نوع بحران کمک گرفت. اگر چه توجه به تقسیم‌بندی انواع بحران‌ها خالی از لطف نیست.

در متون حوزه مدیریت بحران و ارتباطات بحران یکی از موضوعات مورد توجه تقسیم بندی انواع بحران‌ها بر مبنای متغیرهای مختلف است. یکی از تقسیم‌بندی‌های نسبتا جامع را تیموتی کومبز(۲۰۱۲) انجام داده است. کومبز در این دسته‌بندی انواع بحران را بر مبنای علت‌های وقوع آنها از هم متمایز کرده است. کومبز این بحران‌ها را شامل «فجایع طبیعی»، «خشونت در محل کار»، «شایعات»، «بدخواهی»، «حوادث ناشی از خطاهای فنی»، «بازگشت محصولات معیوب»، «خطای انسانی» و «تخلف سازمانی» می‌داند. (بری هوپت و آزودو، ۱۴۰۲: ۷۳-۷۲)

همانگونه که کومبز(۲۰۲۱) بیان کرده است: «ارتباطات بحران یک پدیده جدید نیست» (اوپادهیای[1] و اوپادهیای، ۲۰۲۳: ۱) اما به واسطه گسترش رسانه‌های اجتماعی و رشد بی سابقه سرعت انتقال اخبار منفی مرتبط با بحران‌ها در فضای رسانه های اجتماعی، امروز ارتباطات بحران بیش از پیش مورد توجه قرار گرفته است. به بیان دیگر «اینترنت دارای ویژگی های متعددی است که می تواند باعث ایجاد محیطی مستعد برای بحران گردد» (کراندال، پارنل و اسپیلان، ۱۳۹۶: ۵۵). یکی از جنبه‌هایی که اینترنت را به فضای مناسبی برای ایجاد بحران تبدیل کرده است «وجود گروهی از هکرهای بسیار با انگیزه است» (همان، ۵۶). کومبز در دسته‌بندی بحران‌های مختلفی را زیر مجموعه دسته «بدخواهی» قرار می دهد، به عنوان مثال تروریسم، آدم‌ربایی و هک سیستم‌های اطلاعاتی را جزء این دسته قرار می‌دهد. بنابراین هک شدن سیستم‌های اطلاعاتی سازمان‌ها و شرکت‌ها یکی از مهمترین بحران هایی است که در عصر اینترنت سازمان‌ها با آن مواجه هستند.

طرح مسئله

همانگونه که در مقدمه ذکر شد امروزه بحران‌های اطلاعاتی و امنیتی به بخشی اجتناب‌ناپذیر از مسائل سازمان‌ها و شرکت‌های بزرگ تبدیل شده‌اند. هک داده‌ها یکی از بحران‌های امنیتی مهم است که منجر به نقض گسترده حریم خصوصی کاربران می‌شود. هکرها با اهدافی مانند اخاذی، فروش داده‌ها یا کسب شهرت، سازمان‌های بزرگ را هدف قرار می‌دهند. شرکت‌ها نیز در بحران‌هایی همانند هک از استراتژی‌های مختلف برای اطلاع‌رسانی و اقدامات اصلاحی

---

[1] .Upadhyay

استفاده می‌کنند. این بحران‌ها هم موجب نگرانی‌های گسترده درباره امنیت داده‌ها و حریم خصوصی کاربران می‌شوند و هم ممکن است تأثیرات منفی شدیدی بر اعتبار و وجهه شرکت‌ها داشته باشند. در نتیجه ذی‌نفعان این شرکت‌ها را از اعتماد دوباره به آنها پشیمان کنند و در نهایت سود و درآمد شرکت را به نحو قابل توجهی کاهش می دهد. بنابراین مدیریت این بحران‌ها و استفاده از استراتژی‌های ارتباطات بحران برای شرکت‌ها حیاتی است. در این زمینه، استراتژی‌های ترمیم وجهه نقش حیاتی در بازگرداندن اعتماد عمومی به شرکت‌ها ایفا می‌کنند. بنابراین مسئله این پژوهش استفاده دو شرکت اسنپ فود و تپسی از استراتژی های ارتباطات بحران بعد از هک شدن سامانه های اطلاعاتی آنها برای کاهش آسیب ناشی از بحران و حفظ وجهه شرکت در بین ذی نفعان است، در ادامه به صورت مختصر بحران پیش آمده برای دو شرکت را معرفی خواهیم کرد.

مورد مطالعه اول هک تپسی است که یک شرکت فناوری است که عمدتا در زمینه‌ی تاکسی اینترنتی فعالیت می‌کند. میلاد منشی‌پور مدیرعامل و هم‌بنیان‌گذار تپسی، در روز ۱۱ شهریور ۱۴۰۲ در شبکه اجتماعی ایکس اعلام کرد که در روزهای گذشته یک گروه هکر، به زیرساخت این شرکت دسترسی پیدا کرده که موجب درز بخشی از اطلاعات این مجموعه شده است. منشی‌پور بیان کرد که این گروه قصد اخاذی برای عدم نشر این اطلاعات را داشتند که با مخالفت تپسی، این اطلاعات هم‌اکنون با مبلغ ۳۵ هزاردلار برای فروش گذاشته شده است. او دلیل این مخالفت را اینطور بیان کرد که در مذاکره با گروه هکر متوجه شدند ضمانتی برای عدم انتشار اطلاعات و سواستفاده‌های بعدی وجود ندارد و این عمل، تشویقی برای ادامه این اقدام در مورد سایر شرکت‌ها خواهد بود. (ایکس میلاد منشی‌پور، ۱۴۰۲) در پی این هک گروه هکری در کانال تلگرام خود موارد هک شده را اعلام کرد که شامل اطلاعات بیش از ۲۷ میلیون مسافر شامل نام، شماره همراه، شهر و سایر اطلاعات کاربران بود. همچنین اطلاعات بیش از ۶ میلیون راننده شامل نام، کد ملی، شهر و در نهایت اطلاعات بیش از ۱۳۶ میلیون سفر شامل آدرس کامل مبدا و مقصد بود. (کانال تلگرام IRLeaks، ۱۴۰۲)

مورد دوم مربوط به شرکت اسنپ است که یک شرکت فناوری است و خدمات مختلفی از جمله تاکسی اینترنتی، تحویل غذا، و خرید آنلاین ارائه می‌دهد. اسنپ‌فود -یکی از زیرمجموعه‌های اسنپ- به کاربران امکان سفارش آنلاین غذا، میوه، و سایر مواد غذایی را می‌دهد. بنا بر گزارش سال ۱۴۰۲ اسنپ (سال وقوع هک) تعداد کل کاربران اسنپ‌فود،

۲۰،۴۸۰،۲۱۱ کاربر است. (وب‌سایت اسنپ، ۱۴۰۲) هک اسنپ‌فود در تاریخ ۱۰ دی ۱۴۰۲ بامداد توسط گروه IRLeaks (عامل هک تپسی) اتفاق افتاد. اطلاعات شخصی بیش از ۲۰ میلیون نفر (تقریبا همه کاربران اسنپ‌فود) لو رفت و این گروه اطلاعات را به مبلغ ۳۰ هزار دلار برای فروش گذاشتند و یک نمونه ۱۰۰۰ تایی از اطلاعات را نیز برای اثبات ادعای‌شان منتشر کردند. اطلاعات هک شده شامل نام کاربری، پسورد، ایمیل، نام، شماره موبایل، تاریخ تولد، آدرس کامل بوده است. (وزیری، عباس، ۱۴۰۲) پس از این اتفاق اسنپ‌فود در بیانیه‌ای واکنش نشان داد و همچنین در گزارش سالانه‌ی ۱۴۰۲ به این موضوع پرداخت.

از آنجا که وجهه شرکت‌ها موضوع بسیار مهمی است، شرکت‌ها در بحران‌ها علاوه بر تلاش برای کاهش آسیب‌های بحران از راهبردهای ترمیم وجهه برای طراحی پیام‌های پس از بحران خود استفاده می‌کنند تا از آسیب به وجهه و شهرت خود جلوگیری کنند. (بنت، ۱۹۹۷ و بنت، ۲۰۱۵) در این مطالعه با استفاده از تحلیل مضمون و بررسی واکنش‌های رسانه‌ای اسنپ فود و تپسی پس از بحران تلاش می‌کنیم نشان دهیم چگونه با استفاده از استراتژی‌های ترمیم وجهه پیشنهادی بنت، سعی در کاهش آسیب و بازسازی وجهه خود در بین مشتریان داشتند. بنابراین این پژوهش در پی پاسخ به سه سوال زیر است:

۱. کدام یک از استراتژی‌های ترمیم وجهه در پیام‌های رسانه‌ای اسنپ فود و تپسی بعد از بحران هک سامانه های آنها استفاده شده است؟
۲. استراتژی‌های شرکت‌های تپسی و اسنپ فود چه تفاوتی با یکدیگر دارند؟
۳. واکنش کاربران به این بحران ها چگونه بوده است؟

عملکرد روابط عمومی سازمان‌های دولتی و حتی روابط عمومی شرکت‌های خصوصی در ایران در مواجهه با بحران‌های مختلف بیانگر آن است که استراتژی‌های مشخص و مدونی برای مواجهه با بحران ندارند و به طور خاص در زمینه اطلاع‌رسانی بحران این خلاء و ضعف کاملا مشهود است. بنابراین نتایج این پژوهش می‌تواند به عنوان مرجعی برای دیگر شرکت‌ها و سازمان‌ها در مواجهه با بحران‌های مشابه باشد.

پیشینه پژوهش

در فضای دانشگاهی ایران ارتباطات بحران جزء حوزه هایی است که توجه چندانی به آن صورت نگرفته است، بنابراین طبیعی است که تعداد پژوهش‌های این حوزه هم اندک باشد. در ادامه به اندک تحقیق‌های انجام شده نزدیک به این پژوهش اشاره می‌کنیم.

زهرا اجاق (۱۴۰۱) در پژوهشی با عنوان «شناسایی راهبردهای پاسخ به بحران همه‌گیری کووید ۱۹ در فضای رسانه‌ای ایران» با استفاده از تحلیل مضمون اخبار ساعت ۲۱ و تلویزیون و خبرهای منتشر شده در فضای اینستاگرام به این مسئله پرداخته است که رسانه‌های جریان اصلی(در اینجا تلویزیون) و رسانه‌های غیر رسمی (در اینجا اینستاگرام) از چه راهبردهایی برای پاسخ به بحران استفاده کرده اند. با استفاده از نظریه ارتباطات بحران موقعیتی تیموتی کومبز در نهایت محقق به این نتیجه رسیده است که هم تلویزیون و هم اینستاگرام از چهار راهبرد «چاپلوسی»، «فاصله گذاری»، «رنج» و «سرافکندگی» برای پاسخ به بحران استفاده کرده‌اند. پژوهش اجاق(۱۴۰۱) از جمله تحقیقات اولیه در فضای دانشگاهی ایران است که با ادبیات ارتباطات بحران و به طور خاص نظریه ارتباطات بحران وضعیتی انجام شده است.

اولانیان و همکاران(۲۰۱۴) در پژوهشی با عنوان «کابوس یک گیمر: تحلیل بحران هک پلی استیشن سونی» به بحران هک پلی استیشن سونی پرداخته اند. این بحران نمونه‌ای از سرقت اطلاعات شخصی است که در عصر اطلاعات دیجیتال به طور فزاینده‌ای رایج شده است. این هک نشان‌دهنده نیاز به اقدامات پیشگیرانه برای جلوگیری از چنین بحران‌هایی با هدف حفظ اطلاعات شخصی مشتریان و تضمین اعتماد بین مشتری و فروشنده است. این پژوهش بر ارزیابی هک پلی‌استیشن سونی با استفاده از مدل پیش‌بینی مدیریت بحران (AMCM) تمرکز دارد. با استفاده از اصول AMCM، مشخص شد که شرکت سونی می‌توانست بحران را بهتر مدیریت کند. (Olaniran et al, 2014) بنابراین راهبردهای ارتباطات بحران در بحران‌های این چنینی توسط شرکت‌ها به کار گرفته می‌شود.

روئونن و همکاران(۲۰۲۴) در پژوهشی با عنوان «ارتباطات بحران در مواجهه با نقض داده‌ها» به بررسی استراتژی‌های ارتباطات بحران در مواجهه با نقض داده‌ها و اجرای عملی آن‌ها می‌پردازد. این پژوهش بر پایه مطالعات پویا در حوزه ارتباطات بحران بنا شده است. همانطور که چند مطالعه کیفی در فنلاند نشان داده‌اند که اصول متعارف همچنان معتبر هستند؛ در موارد موفق، سازمان‌ها اطلاع‌رسانی سریع، پذیرش مسئولیت، ارائه عذرخواهی و اطلاع‌رسانی به نهادهای عمومی را در پیش گرفته‌اند. در مقابل، موارد ناموفق شامل مواردی چون مقصر دانستن دیگران، معرفی سازمان به‌عنوان قربانی، و عدم اطلاع‌رسانی به مقامات عمومی بوده‌اند. (Ruohonen et al, 2024)

نایت و نرس(۲۰۲۲) در پژوهشی با عنوان «چارچوبی برای ارتباطات موثر سازمانی پس از حوادث امنیت سایبری» به بررسی انتقادی و چندوجهی، اثربخشی ارتباطات بحران و روابط عمومی پس از نقض داده‌ها را تحلیل می‌کند. در این پژوهش برای تفسیر و ساختاربندی نتایج، از تحلیل داده‌های کیفی استفاده شده که به توسعه یک چارچوب جامع جدید برای ارتباطات شرکتی کمک می‌کند تا شرکت‌ها را در آماده‌سازی و واکنش به چنین رویدادهایی یاری دهد. اعتبار این چارچوب از طریق ارزیابی آن در مصاحبه با متخصصان ارشد صنعت و همچنین بررسی انتقادی در مقایسه با تحقیقات و شیوه‌های مرتبط سنجیده شده است. این چارچوب نخستین پیشنهاد جامع و ارزیابی‌شده برای شناسایی ارتباطات شرکتی مؤثر پس از رخدادهای امنیت سایبری محسوب می‌شود و بر اساس آن برای مدیریت بحران ناشی از نفوذ داده‌ها، سازمان‌ها باید واکنش مناسبی داشته باشند. مثلا پس از بحران ابتدا کارکنان را فراخوانی[1] کرده و منابع کافی برای رسانه‌های اجتماعی و مراکز تماس فراهم کنند. همچنین، ظرفیت سامانه‌های ارتباطی را افزایش داده و انتقال تراکنش‌ها به کانال‌های امن را پیش‌بینی نمایند. در ارسال پیام، وضوح و سادگی اهمیت دارد. استفاده از اصطلاحات پیچیده باید اجتناب شود تا پیام به‌روشنی قابل‌درک باشد. این امر موجب حفظ اعتماد عمومی می‌شود. علاوه بر این، باید آمادگی لازم برای پاسخ‌گویی به رسانه‌ها وجود داشته باشد، افت احتمالی ارزش سهام در روزهای نخست پیش‌بینی شود، و اقدامات مقابله با حملات فیشینگ انجام گیرد. همچنین، مدیرعامل یا رئیس سازمان باید پیام را ارائه دهد تا نشان دهد سازمان بحران را جدی گرفته و از تشدید غیرضروری آن جلوگیری کند. (Knight & Nurse, 2020)

کوییرز و شونهایت(۲۰۲۱) در پژوهشی با عنوان «نقض داده‌ها و ارتباطاتت موثر بحران: تحلیل مقایسه بحران‌های اعتبار سازمانی» به مطالعه‌ی نقض داده‌های آنلاین پرداخته‌اند. نقض‌های داده‌های آنلاین حوادث سایبری مکرر و آسیب‌رسانی هستند که سازمان‌های سراسر جهان با آن‌ها مواجه می‌شوند. این مطالعه بررسی می‌کند که چگونه سازمان‌ها می‌توانند با استفاده از استراتژی‌های ارتباطات بحران موقعیتی، به طور مؤثری آسیب‌های وجهه‌ای را در پی نقض‌های داده توسط هک کاهش دهند. بحران‌های نقض داده‌های مشابه تأثیر منفی یکسانی بر وجهه سازمانی ندارند. واکنش‌های پایه‌ای مانند ارائه دستورالعمل‌های جامع و کامل و توضیحات دقیق در مورد حادثه به مصرف‌کنندگان، به کاهش آسیب کمک کردند. شرکت‌هایی

---

[1] brief

که در پاسخ به نقض‌های داده‌های توسط هک، مسئولیت را پذیرفتند، با وجود اینکه چنین بحران‌هایی به عنوان نوع بحران‌های قربانی تعریف می‌شوند، بهره‌مند شدند. سازمان‌هایی که عمدتاً به یک استراتژی واحد تکیه کردند، عملکرد بهتری نسبت به آن‌هایی داشتند که استراتژی‌ها را به طور ناسازگار مخلوط کردند. به طور خاص، انکار در نهایت به وجهه سازمانی آسیب زد. خودافشایی به شرکت‌ها اجازه داد تا تأثیر مثبتی بر گزارش‌های رسانه‌ای بگذارند. ارتباطات رسانه‌های اجتماعی نقش مهمی در پاسخ سازمان‌های درگیر نداشت. پذیرش مداوم و به موقع استراتژی‌های جبران، عذرخواهی و اصلاح، همراه با استراتژی‌های تقویتی مانند تحسین و تقویت، بهبودی وجهه از بحران را به طور مثبتی تحت تأثیر قرار داد. (Kuipers & Schonheit, 2021) نتایج این مطالعه می‌تواند به اتخاذ استراتژی‌های مناسب توسط شرکت‌ها در هنگام بحران‌های سایری کمک کند. نکته‌ی دیگر آن است که نقض‌های داده (توسط هک) به طور متوسط در موقعیت بین نوع بحران قربانی و بحران قابل پیشگیری قرار می‌گیرند و در دسته بحران‌های اتفاقی قرار می‌گیرند که فرض می‌شود دارای کنترل‌پذیری مستقیم پایین و بدون عمدیت هستند. موضع پاسخ سازمان به رخنه‌های داده (توسط هک) ابتدا باید به واکنش‌های پایه‌ای (تعدیل و آموزش) متکی باشد، و سپس با استفاده از استراتژی‌های کاهش یا بازسازی همراه شود. (Kuipers & Schonheit, 2021).

پارک (۲۰۱۷) در پژوهشی با عنوان «راهبردهای موثر پاسخ به بحران» نیز دریافته که اثر واکنش‌های پایه‌ای به عنوان بخشی از استراتژی ارتباطات به طور واقعی تاکنون کم‌تر مورد مطالعه قرار گرفته است، حتی با این که این واکنش‌ها برای همه بحران‌ها لازم هستند (Park, 2017).

بنتلی و همکاران(۲۰۱۸) در پژوهشی با عنوان «متاسفیم اما ما مقصر نیستیم: عذرخواهی‌های سازمانی در شرایط بحرانی مبهم» ادعا می‌کنند که سازمان‌هایی که دچار رخنه‌های داده می‌شوند، اغلب از پذیرش مسئولیت در بحران‌های مرتبط با نقض داده‌ها سر باز می‌زنند احتمالا آنجا که نقض داده‌ها معمولاً به هکرها نسبت داده می‌شود و دلیلی وجود ندارد که سازمان مسئولیت را بپذیرد. همچنین استراتژی همدلی در شرایطی که سازمان به وضوح مقصر بود، بیشتر از زمان وقوع بحران‌های مربوط به نقض داده‌ها مشاهده شد. (Bentley et al. 2018)

مرور پژوهش‌های اندک جامعه ایران و پژوهش‌های خارجی بیانگر آن است که هک سیستم‌های اطلاعاتی سازمان‌ها یکی از جدی ترین بحران‌هایی است که سازمان ها در عصر اینترنت با آن مواجه هستند، در فضای دانشگاهی ایران تاکنون پژوهشی منتشر نشده است که

از زاویه ارتباطات بحران و به طور خاص نظریه ترمیم وجهه هک سیستم های اطلاعاتی سازمان‌ها را مورد توجه قرار دهد، بنابراین این پژوهش می‌تواند آغازی برای توجه به راهبردهای پاسخ به بحران و به طور خاص استفاده از نظریه ترمیم وجهه برای استفاده سازمان در شرایط بحرانی باشد. در فضای جهانی اما تعداد پژوهش هایی که با راهبردهای ترمیم وجهه به مطالعه عملکرد سازمان ها در شرایط بحران بپردازند بی شمار است، اما وجهه تمایز این پژوهش با فضای تحقیقات ارتباطات بحران در عرصه جهانی می‌تواند این باشد که آیا این راهبردها فارغ از فضای فرهنگی جوامع قابل استفاده هستند یا خیر.

ادبیات نظری

برای آن که به ارتباطات بحران در سازمان‌ها بپردازیم، پرداختن به معنای بحران لازم است. می‌توان گفت بحران‌ها شامل پیامدهای بالا برای عملیات و شهرت سازمانی هستند؛ می‌توانند یک رویداد ساده یا پیچیده یا مجموعه‌ای از رویدادها که هم‌زمان اتفاق می‌افتند باشند؛ بحران‌ها از نوع اتفاقات غافلگیرکننده هستند که ذاتاً قابل‌پیش‌بینی نیستند؛ بحران‌ها به طور واقعی یا ادراکی عملکرد یا تصور عمومی را تهدید می‌کنند؛ و بحران‌ها نیازمند فرآیند ساخت معنا در سازمان‌ها هستند تا سطح عدم قطعیت کاهش یافته و ثباتی برقرار شود که به بقای سازمانی کمک کند.(Spradley, 2017)

حالا بیشتر سازمان‌ها در بخش‌های خصوصی و عمومی شروع به تخصیص منابع برای جلوگیری، آمادگی و مدیریت انواع مختلف بحران کرده‌اند. بدون شک، دنیای کسب‌وکار مدت‌ها است که تحت تأثیر بحران‌ها و رسوایی‌های طولانی است، اما در دهه ۱۹۸۰ مدیریت بحران و ارتباطات بحران وارد دستورکار سازمانی به عنوان یک رویه سازمانی خاص شد. (Frandsen & Johansen ,2016)

استراتژی‌های پاسخ به بحران یک سازمان از طریق آنچه که سازمان می‌گوید و چگونگی عمل سازمان در زمان بحران بررسی می‌شوند. بحران‌های قبلی که برای سازمان اتفاق افتاده‌اند نیز وجهه سازمان را تحت تاثیر قرار داده و شدت تهدید وجهه سازمان را افزایش دهند، به علاوه تأثیر بحران بر اعتبار سازمان بیشتر مستقیم بوده و ناشی از برداشت عمومی از مسئولیت سازمان در بحران است، نه اثرات غیرمستقیم آن. (Coombs, 2004).برای مدیریت موثر بحران، نظریه‌ها و مدل‌های مختلفی ارائه شده‌اند که هر یک تعدادی از استراتژی‌های پاسخ به بحران را پیشنهاد می‌کنند. نظریه ترمیم وجهه بنت (۱۹۹۷) نیز یکی از این نظریه‌هاست که یک

چارچوب استراتژیک جامع برای کارشناسان فراهم می‌کند. بر پایه‌ی کار Ware و Linkugel (۱۹۷۳) و ادبیات Scott و Lyman (۱۹۶۸)، بنت نظریه‌ای جامع درباره‌ی بازیابی وجهه یا ترمیم وجهه توسعه داد. وجهه به چگونگی ادراک سازمان توسط ذینفعان و یا عموم مردم اشاره دارد. پنج استراتژی اصلی شامل انکار، طفره رفتن از مسئولیت، کاهش آسیب رویداد، اقدام تصحیحی و تاسف و شرمساری هستند. این فرآیند برای پاسخگوئی به افکار عمومی یا سازمان‌ها در مواجهه با شکایات یا اقدامات متقابل طراحی شده است. در واقع استراتژی‌های ترمیم وجهه بنت بر نحوه واکنش سازمان‌ها به اتهامات یا پاسخگویی به اقدامات خود پس از متهم شدن به تخلف متمرکز است و یک واکنش موثر برای ترمیم وجهه آسیب دیده سازمان طراحی کرده است. (O'Hair & L. Heath, 2010) استراتژی‌ها در جدول زیر بیان شده‌اند. این استراتژی‌ها نشان می‌دهند که چگونه سازمان‌ها و افراد می‌توانند به طور موثر به بحران پاسخ دهند تا تصویر آسیب‌دیده خود را بازسازی کنند.

جدول ۱: استراتژی های ترمیم وجهه مدل بنت

استراتژی	انواع	ویژگی‌های کلیدی
انکار[۱]	انکار ساده[۲]	عمل انجام نشده
	تغییر مقصر[۳]	عمل توسط دیگری انجام شده
طفره رفتن از مسئولیت[۴]	تحریک[۵]	پاسخ به عمل دیگری
	ناتوانی[۶]	کمبود اطلاعات یا توانایی
	تصادف[۷]	عمل اشتباه بود
	نیت خوب[۸]	نیت خوب در عمل
کاهش آسیب رویداد[۹]	تقویت[۱۰]	تأکید بر ویژگی‌های خوب
	کوچک‌نمایی[۱۱]	عمل جدی نیست
	تمایز[۱]	عمل کمتر تهاجمی است

[1] Denial
[2] Simple Denial
[3] Shift the Blame
[4] Evasion of Responsibility
[5] Provocation
[6] Defeasibility
[7] Accident
[8] Good Intentions
[9] Reducing Offensiveness of Event
[10] Bolstering
[11] Minimization

استراتژی	انواع	ویژگی‌های کلیدی
	تعالی[۲]	ملاحظات مهم‌تر
	حمله به متهم[۳]	کاهش اعتبار متهم
	جبران[۴]	غرامت دادن به قربانی
اقدام تصحیحی[۵]	_	برنامه‌ریزی برای حل یا جلوگیری از تکرار مشکل
تاسف و شرمساری[۶]	_	عذرخواهی برای عمل

منبع: (Benoit, 1997)، (Zhang & Benoit, 2004)

انکار

یکی از رویکردهای عمومی برای ترمیم وجهه، با دو نوع مختلف، انکار است. یک شرکت می‌تواند انکار کند که این عمل رخ داده، شرکت آن عمل را انجام داده، یا این عمل به کسی ضرر رسانده است. دومین شکل انکار، انتقال تقصیر است؛ به این معنا که ادعا می‌شود شخص یا سازمان دیگری در واقع مسئول عمل تهاجمی است (Benoit, 1997).

طفره رفتن از مسئولیت

این استراتژی ترمیم وجهه عمومی چهار نسخه دارد. یک شرکت می‌تواند بگوید که عمل آن صرفاً پاسخی به عمل تهاجمی دیگران بوده است و این رفتار را می‌توان به‌عنوان واکنش منطقی به تحریک آن دانست. به‌عنوان مثال، یک شرکت می‌تواند ادعا کند که کارخانه خود را به ایالت دیگری منتقل کرده است زیرا ایالت اول قانونی جدید تصویب کرده که حاشیه سود آن را کاهش داده است. یک شکل خاص دیگر از طفره رفتن از مسئولیت، قابلیت نقص و ناتوانی است. در اینجا، شرکت ادعا می‌کند که فاقد اطلاعات یا کنترل بر عناصر مهم وضعیت است. به عنوان مثال، یک مدیر اجرایی مشغول که یک جلسه مهم را از دست داده است می‌تواند ادعا کند که "من هرگز مطلع نشدم که جلسه به روز دیگری منتقل شده است." اگر درست باشد، کمبود اطلاعات غیبت را توجیه می‌کند. گزینه سوم بیان این ادعا است که عمل تهاجمی به طور تصادفی رخ داده است. اگر شرکت بتواند مخاطبان را قانع کند که عمل مورد نظر به طور

---

[1] Differentiation
[2] Transcendence
[3] Attack Accuser
[4] Compensation
[5] Corrective Action
[6] Motification

تصادفی رخ داده است، باید کمتر پاسخگو باشد و آسیب به وجهه آن شرکت کاهش یابد. مثلا بیان این که اشتباهات غیر عمدی بوده است. چهارم، شرکت می‌تواند پیشنهاد کند که رفتار تهاجمی با نیت خوب انجام شده است (Benoit, 1997).

کاهش آسیب رویداد

یک شرکت که متهم به اعمال نادرست شده است، می‌تواند تلاش کند تا ادراک تهاجم از آن عمل را کاهش دهد. این استراتژی ترمیم وجهه عمومی شش نسخه دارد. ابتدا، یک شرکت می‌تواند از تقویت استفاده کند تا احساسات مثبت مخاطبان را نسبت به خود تقویت کند، به‌منظور جبران احساسات منفی مرتبط با عمل نادرست. شرکت‌ها ممکن است ویژگی‌های مثبت خود یا اعمال مثبتی که در گذشته انجام داده‌اند را توصیف کنند. دومین امکان، تلاش برای کاهش احساسات منفی مرتبط با عمل نادرست است. مثلا ممکن است مسئولان تلاش کنند میزان آسیب را کم اهمیت جلوه دهند. این کار به کاهش مشکل ظاهری کمک می‌کند. سوم، یک شرکت می‌تواند از تمایز استفاده کند، که در آن عمل از اعمال مشابه اما تهاجمی‌تر متمایز می‌شود. مثلا وقتی اعمال شرکت به‌عنوان نگهداری پیشگیرانه درک شوند و نه به‌عنوان تقلب، بسیار کمتر تهاجمی به‌نظر می‌رسند. چهارمین روش برای کاهش تهاجم، تعالی است، که تلاش می‌کند عمل را در یک زمینه مطلوب‌تر قرار دهد. یک شرکت که بر روی حیوانات آزمایش می‌کند، می‌تواند ادعا کند که منافع حاصل از این تحقیق برای انسان‌ها بیشتر از ضررهای وارد به حیوانات است. پنجم، کسانی که متهم به اعمال نادرست شده‌اند ممکن است تصمیم بگیرند که به متهمان خود حمله کنند. و در نهایت غرامت دادن شکل نهایی کاهش تهاجم است. اگر این امر برای قربانی قابل قبول باشد، وجهه شرکت باید بهبود یابد. به‌عنوان مثال، یک گروه از افراد دارای معلولیت از ورود به یک سینما منع شدند. یک مقام بعداً عذرخواهی کرد و به آن‌ها بلیت‌های رایگان برای یک فیلم آینده پیشنهاد داد تا این عمل تهاجمی را جبران کند (Benoit, 1997).

اقدام تصحیحی

یکی دیگر از استراتژی‌های ترمیم وجهه عمومی، اقدام تصحیحی است، که در آن شرکت قول می‌دهد مشکل را برطرف کند. این اقدام می‌تواند به‌صورت بازگرداندن وضعیت موجود قبل از عمل تهاجمی و/یا قول جلوگیری از تکرار عمل تهاجمی در آینده باشد (Benoit, 1997).

تأسف و شرمساری

آخرین استراتژی عمومی برای ترمیم وجهه، تاسف، شرمساری، اعتراف و طلب بخشش است. یکی از معایب احتمالی این استراتژی این است که ممکن است قربانیان را به طرح دعوی قضایی دعوت کند (Benoit, 1997).

نظریه ترمیم وجهه قبل از ظهور اختلالات رسانه‌های جدید ایجاد شد، همانطور که مجموعه‌ای از استراتژی‌های پاسخ به بحران پیشنهادی با تمرکز بر بازسازی تصویر آسیب‌دیده سازمان از بحران، به طور گسترده‌ای برای دهه‌ها در بحران‌ها استفاده می‌شده است. (Chon & Kim, 2022).

رسانه‌های اجتماعی چندین مزیت خاص در اختیار پژوهشگران بحران گذاشته‌اند تا استفاده از استراتژی‌های ترمیم وجهه به عنوان شواهدی در پیام‌های ارتباطی عمومی سازمان‌های آسیب‌دیده از بحران را مطالعه کنند. (Kamboh et al.,2023) اخیرا این رسانه‌ها مانند توییتر و فیسبوک، نسبت به تکنولوژی‌های ارتباطی قبلی ابزارهای مهم‌تری در ارتباطات بحران هستند (Sellnow & Seeger, 2013)

و میتوان گفت رسانه‌های اجتماعی به عنوان مکان‌های اصلی برای ارتباط دادن تلاش‌های ترمیم وجهه برای افراد و سازمان‌ها جایگزین رسانه‌های سنتی شده‌اند (Allison et al.,2020). ویژگی تعاملی رسانه‌های اجتماعی به صورت لایک، اشتراک‌گذاری، نظر دادن و ... به سازمان‌ها این امکان را می‌دهد که به طور باز، سریع، صادقانه، حقیقی و مستقیم با گروه‌های مختلف مخاطبان ارتباط برقرار کنند. استفاده از فناوری‌های اینترنتی می‌تواند به شفافیت سازمانی و شفافیت سیاست‌گذاری، تعامل میان سازمان‌ها و بخش‌های سیاست‌گذاری، و ایجاد سیاست‌ها و فرایندهای نوآورانه کمک کند. کاربران رسانه‌های اجتماعی نه تنها مطالب را می‌خوانند، بلکه به استراتژی‌های ترمیم وجهه پاسخ می‌دهند، حتی چندین بار، و با دیگران در مورد مسائل بحران بحث می‌کنند (Howard, 2020). این مسائل نه تنها برای یک سازمان درگیر در بحران مهم است بلکه برای پژوهشگران بحران نیز اهمیت دارد تا مسائل عمده را در نظرات کاربران رسانه‌های اجتماعی شناسایی کرده و گفتمان عمومی گسترده‌تری را در مورد این مسائل ارزیابی کنند. در شبکه‌های اجتماعی می‌توان با سرعت بالایی به بحران واکنش نشان داد و همانطور که بنت می‌گوید بازسازی یک سازمان به طور عمده بستگی به این دارد که چقدر سریع به بحران پاسخ می‌دهد (Benoit, 1997).

با توجه به این ویژگی‌های مهم و موثر رسانه‌های اجتماعی و در راستای مطالعات قبلی در ارتباطات بحرانی سازمانی مبتنی بر رسانه‌های اجتماعی، شناسایی اینکه کدام استراتژی‌های

خاص ترمیم وجهه در بحران توسط اسنپ استفاده شده است، مفید است. بنابراین سوال تحقیقاتی اصلی این مطالعه کشف استراتژی‌های پاسخ به بحران استفاده شده توسط اسنپ برای راضی کردن کاربران پس از هک مطرح شده است.

روش تحقیق

در این پژوهش ما از روش تحلیل محتوای نظریه‌محور استفاده کردیم که یکی از روش‌های متداول برای تحلیل متن‌های رسانه‌ای است. بنابراین موارد نظریه بنت را مورد توجه قرار داده و محتوا را متناسب با آن مورد تحلیل قرار داده‌ایم.

ما مجموعه ای از داده ها را برای مطالعه‌ی استراتژی‌های ارتباطات بحران این دو شرکت مورد بررسی قرار داده ایم، این داده ها شامل: (۱) توییت‌های ایکس تپسی و اسنپ‌فود (۲) پست‌های اینستاگرامی تپسی، اسنپ و اسنپ‌فود (۳) اطلاعیه‌ها و محتوای منتشر شده در سایت اسنپ فود و تپسی ۴. اطلاعیه های گروه تلگرامی گروه هکری ۵. توییت های کاربران در پاسخ به واکنش های تپسی و اسنپ فود

در این مطالعه تمام توییت‌ها، پست‌های اینستاگرامی و محتوای وب‌سایت‌ها را از تاریخ هک (۱۱ شهریور ۱۴۰۲ برای تپسی و ۱۰ دی ۱۴۰۲ برای اسنپ) تا تاریخ نگارش مقاله (۱۵ اسفند ۱۴۰۳) جستجو کردیم. در نهایت رشته توییت میلاد منشی‌پور (بنیانگذار تپسی) به عنوان واکنش قابل استناد تپسی مورد مطالعه قرار گرفت. درباره اسنپ فود توییت حساب کاربری اسنپ‌فود و گزارش سالانه شرکت اسنپ در سال ۱۴۰۲ به عنوان واکنش قابل استناد مورد مطالعه قرار گرفت. البته کل توییت‌های این دو اکانت مربوط به بازه‌ی زمانی هک بررسی شد، همچنین تمام پست‌های اینستاگرام بازه‌ی زمانی هک نیز بررسی شدند اما این شرکت‌ها در حساب اینستاگرام‌شان اشاره‌ای به هک نکرده بودند.

سپس با استفاده از استراتژی‌های ترمیم وجهه که در نظریه ترمیم وجهه بنت (۱۹۹۷) توضیح داده شده است، دسته‌های ساخته شده را به شرح زیر عملیاتی کردیم:

دسته ۱: انکار

این دسته شامل تمام واحدهای تحلیلی است که در آن‌ها «تیم سرویس آنلاین» به سادگی هرگونه بحران در سازمان را انکار کرد؛ یا تقصیر بحران را به دلایل دیگر منتقل کرد.

دسته ۲: طفره رفتن از مسئولیت

این دسته شامل واحدهای تحلیلی است که برای متقاعد کردن مخاطبان مبنی بر اینکه سرویس مسئولیتی در قبال هک ندارد استفاده شدند.

دسته ۳: کاهش آسیب

این دسته شامل تمام واحدهای تحلیلی است که برای کاهش میزان احساسات منفی مخاطبان ارسال شده‌اند، مثلاً یادآوری اقدامات مثبت انجام شده در گذشته یا حال (تقویت)؛ مشکل کمی ایجاد شده است (کمینه سازی) در شرایط مشابه نامطلوب، بسیاری از اپلیکیشن‌ها با شرایط مشابهی روبرو هستند و این اتفاقات در تمام دنیا می‌افتد (تمایز)؛ این هک در نهایت ما را به سمتی برد که بیشتر مواظب امنیت حریم خصوصی شما باشیم. (تعالی)؛ متهم کردن هکرها (حمله به متهم)؛ سرویس از این به بعد امن‌تر خواهد بود (جبران)

دسته ۴: اقدام تصحیحی

این دسته شامل واحدهای تحلیلی است که برای بازگرداندن وضعیت امور موجود قبل از بحران هک یا وعده جلوگیری از تکرار آن در آینده با انجام اقدامات تصحیحی لازم ارسال شده است.

دسته ۵: تاسف

این دسته شامل هر واحد تحلیلی است که مسئولیت بحران را پذیرفته و از مخاطبان طلب عفو کرده است.

سپس محتوا توسط پژوهشگران مورد تحلیل قرار گرفت و با تحلیل مضمون محتواها استراتژی‌های موجود در این محتواها بر اساس دسته‌بندی‌های گفته شده استخراج شدند. همچنین برای پاسخ به سوال دیگر مطالعه در خصوص واکنش کاربران، ما واکنش کاربران را از طریق تحلیل محتوای داده‌محور سنجیده‌ایم. بدین منظور پاسخ‌های کاربران به توییت میلاد منشی‌پور و توییت اسنپ‌فود مورد بررسی قرار گرفت. این پاسخ‌ها که در قالب توییت منتشر شده‌اند، ما آنها را استخراج و تحلیل کردیم. مجموعا پس از حذف موارد نامرتبط ۱۳۱ توییت در پاسخ به منشی‌پور و ۱۵۷ توییت در پاسخ به اسنپ‌فود مطالعه شد. از آنجا که پست‌های اینستاگرامی مجزایی با موضوع هک توسط صفحات شرکت‌ها منتشر نشده بود، بنابراین واکنش کاربران در اینستاگرام مورد مطالعه قرار نگرفته است.

همچنین۱۰ اطلاعیه گروه هکری در کانال تلگرام IRLeaks هم برای دستیابی به نتایج دقیق‌تر مورد تحلیل قرار گرفتند.

یافته‌ها

با تحلیل پیام‌های رسانه‌ای منتشر شده پس از هک توسط دو پلتفرم تپسی و اسنپ فود، یافته‌های زیر به دست آمد:

جدول ۲: استراتژی‌های تپسی

پلتفرم تپسی			
فضای ارتباطی	**استراتژی استفاده شده**	**نمونه**	**تحلیل**
ایکس میلاد منشی‌پور (بنیانگذار تپسی)	انکار: تغییر مقصر	طی روزهای گذشته، متوجه دسترسی غیرمجاز به زیرساخت شرکت تپسی و برداشت بخشی از اطلاعات شدیم.	اشتباهی از سمت شرکت اتفاق نیفتاده، مقصر گروه هکری است.
ایکس میلاد منشی‌پور (بنیانگذار تپسی)	طفره رفتن از مسئولیت: نیت خوب	ما تصمیم گرفتیم که به این اخاذی تن ندهیم، چرا که در مذاکره با آنها متوجه شدیم که نه تنها ضمانتی برای عدم نشر اطلاعات و سواستفاده‌های آتی وجود ندارد بلکه تشویقی برای ادامه‌ی این اقدام در مورد سایر شرکت‌ها نیز خواهد بود.	اگرچه مسئولیت شرکت آن است که از درز اطلاعات حتی با خرید آنها جلوگیری کند، اما از این مسئولیت به دلیل تمایل به جلوگیری از سوءاستفاده‌های آتی شانه خالی می‌کند.
ایکس میلاد منشی‌پور (بنیانگذار تپسی)	کاهش آسیب: تعالی	ما تصمیم گرفتیم که به این اخاذی تن ندهیم، چرا که در مذاکره با آنها متوجه شدیم که نه تنها ضمانتی برای عدم نشر اطلاعات و سواستفاده‌های آتی وجود ندارد بلکه تشویقی برای ادامه‌ی این اقدام در مورد سایر شرکت‌ها نیز خواهد بود.	شرکت برای جلوگیری از درز اطلاعات مبلغی به گروه هکری نپرداخته ولی این کار را برای این انجام داده که جلوی سوءاستفاده‌ها را به طور کل بگیرد.
ایکس میلاد منشی‌پور (بنیانگذار تپسی)	اقدام تصحیحی	به محض کشف این موضوع، ضمن ثبت شکایت، پلیس را در جریان قرار دادیم و راه دسترسی آنها را بستیم.	شکایت به عنوان اقدام تصحیحی بیان شده در صورتی که نمی‌توان با شکایت درز اطلاعات را از بین برد. بستن دسترسی هکرها نیز تنها می‌تواند از خطرهای احتمالی بعدی جلوگیری کند.
ایکس میلاد منشی‌پور	اقدام تصحیحی	مسئولیت آن را می‌پذیرم و حتما بررسی دقیقی در مورد	اقدام تصحیحی شرکت در ارتباط با کاربران بررسی و گزارش آتی

پلتفرم تپسی			
فضای ارتباطی	استراتژی استفاده شده	نمونه	تحلیل
(بنیانگذار تپسی)		دلایل وقوع آن انجام خواهم داد. متعاقبا گزارش این بررسی را اعلام خواهم کرد.	است. البته این گزارش هرگز در صفحه‌ی منشی‌پور منتشر نشده است.
ایکس میلاد منشی‌پور (بنیانگذار تپسی)	تاسف	در انتها، بابت این اتفاق متاسفم، مسئولیت آن را می‌پذیرم...	اگرچه عذرخواهی صورت گرفته اما بسیار کوتاه است، هیچ ابراز احساسات و برانگیختن همدلی دیده نمی‌شود و عذرخواهی در پایان متن قرار گرفته.

جدول ۳: استراتژی‌های اسنپ

پلتفرم اسنپ			
فضای ارتباطی	استراتژی استفاده شده	نمونه	تحلیل
ایکس اسنپ‌فود	کاهش آسیب: کوچک‌نمایی	لازم به ذکر است که کلیه‌ی اطلاعات پرداخت بانکی کاربران، اعم از اطلاعات مربوط به کد امنیتی کارت (CCV)، رمز عبور و تاریخ انقضا، در امنیت کامل قرار دارد و این اطلاعات مطابق مقررات بانک مرکزی در هیچ یک از پلتفرم‌ها ذخیره نمی‌شود.	از بین تمام اطلاعات هک شده تنها موارد مربوط به اطلاعات پرداخت بانکی طبق ادعای اسنپ‌فود امن هستند و اشاره‌ای به سایر اطلاعات مانند آدرس نشده است که اتفاقا اهمیت بالایی دارند. ضمنا در اطلاعیه با بی‌دقتی به جای CVV2، کلمه CCV نوشته شده که اگرچه اشتباه نیست اما کاربرد آن در ایران اصلا مرسوم نیست. این موضوع اعتبار ادعای ذکر شده را نیز کاهش می‌دهد همانطور که کاربران نیز به عنوان اشتباه آن اشاره کرده‌اند.
ایکس اسنپ‌فود	کاهش آسیب: حمله به متهم	گفتنی است این گروه هکری پیش از مذاکره با اسنپ‌فود اقدام به فروش اطلاعات کرده است.	گروه هکری بدون مذاکره اطلاعات را به فروش گذاشته، پس گروه هکری مقصر است و اقدام نادرستی داشته.
ایکس اسنپ‌فود	اقدام تصحیحی	پیرو هک و اقدام به فروش مستقیم بخشی از اطلاعات کاربران اسنپ‌فود به اطلاع می‌رسانیم که شرکت اسنپ‌فود در قدم اول در همکاری با پلیس فتا در حال شناسایی و رفع منبع آلودگی ناشی از اقدام این گروه هکری است.	شرکت در قدم اول صرفا به همکاری با پلیس و رفع منبع آلودگی اکتفا کرده که هیچ کدام جلوی درز اطلاعات مشتریان را نمی‌گیرد.
ایکس	اقدام تصحیحی	شرکت اسنپ‌فود مسئولیت این اتفاق را	بررسی به عنوان اقدام تصحیحی

پلتفرم اسنپ			
فضای ارتباطی	استراتژی استفاده شده	نمونه	تحلیل
اسنپ‌فود		می‌پذیرد و حتما بررسی دقیقی در مورد دلایل وقوع آن انجام خواهد داد.	مشابه کاری است که تپسی انجام داده بود. این بررسی نفعی برای بازگرداندن اطلاعات ندارد.
ایکس اسنپ‌فود	اقدام تصحیحی	شرکت اسنپ‌فود حداکثر تلاش خود را برای جلوگیری از انتشار داده‌های کاربران، از طریق مذاکره با این گروه هکری، خواهد کرد.	از مذاکره به عنوان اقدام تصحیحی یاد شده که با توجه به این که بیان شده هکرها قبل از مذاکره اقدام به فروش کرده‌اند متناقض به نظر می‌رسد.
ایکس اسنپ‌فود	اقدام تصحیحی	متعاقبا اطلاعات تکمیلی در این مورد را منتشر خواهیم کرد.	از بیان اطلاعات تکمیلی یاد شده است که انتظار می‌رفت بیانیه‌ی دیگری منتشر شود یا اطلاعات بیشتری بیان شود اما تنها اطلاعات منتشره‌ی متعاقب گزارش سال اسنپ در ۱۴۰۲ است که شفافیت بیشتری درباره اتفاقی که افتاده ندارد.
وب‌سایت اسنپ (گزارش ۱۴۰۲)	کاهش آسیب: تقویت	این حادثه آموزه‌های بسیاری را به دنبال داشت و فصل جدیدی در امنیت سایبری گروه اسنپ رقم زد.	اسنپ بیان کرده که در پی این هک امنیت سایبری خود را بالا برده است. اگرچه موارد تقویت به طور جزئی در سایت ذکر نشده اما در فایل گزارش کامل که از سایت قابل دانلود است مواردی مانند امکان حذف حساب کاربری یا برنامه‌ریزی برای رمزنگاری داده‌ها ذکر شده. این گزارش کامل به دلیل آن که به طور مستقیم در سایت یا شبکه‌های اجتماعی بیان نشده در دسترس عموم مخاطبان نیست.
وب‌سایت اسنپ (گزارش ۱۴۰۲)	کاهش آسیب: تعالی	بهبود و ارتقای تمهیدات امنیتی مسیری بی‌پایان و نیازمند تفکر پویا و پیوسته درباره‌ی راهکارهای امنیتی و پیش‌بینی روندهاست. این مسیر تنها با پذیرش و درک عمیق از روش‌های حمله و آسیب‌پذیری‌های مختلف، آگاهی‌رسانی و آموزش کارکنان، به‌روزرسانی سیستم‌ها و نرم‌افزارها، استفاده از تکنولوژی‌های روز و تشکیل تیم‌های	فحوای بیان این است که تنها راه برای بهبود و ارتقای تمهیدات امنیتی تجربه‌ی آسیب‌هایی مانند هک است. بنابراین هک در نهایت منجر به این شده که امنیت سایبری اسنپ بهبود یابد.

پلتفرم اسنپ			
فضای ارتباطی	استراتژی استفاده شده	نمونه	تحلیل
		متخصص امنیت سایبری طی می‌شود.	
وب‌سایت اسنپ (گزارش ۱۴۰۲)	اقدام تصحیحی	اوایل زمستان ۱۴۰۲، گروهی هکری از دسترسی به اطلاعات کاربران اسنپ‌فود خبر داد. اسنپ‌فود ضمن پذیرش مسئولیت این موضوع در مذاکره‌ای موفقیت‌آمیز با این گروه هکری از انتشار اطلاعات کاربران جلوگیری کرد.	اسنپ‌فود در گزارش اعلام کرده که از انتشار اطلاعات کابران جلوگیری کرده است. می‌توان گفت با فرض صحت این ادعا، این مورد یک اقدام تصحیحی واقعی است.

مقایسه واکنش اسنپ و تپسی به هک شدن، به این شرح است:

جدول ۴: مقایسه واکنش‌های اسنپ فود و تپسی به هک سامانه های اطلاعاتی آنها

استراتژی	نوع	پلتفرم
انکار	تغییر مقصر	تپسی
طفره رفتن از مسئولیت	نیت خوب	تپسی
کاهش آسیب	تقویت	اسنپ فود
	کوچک‌نمایی	اسنپ فود
	تعالی	تپسی – اسنپ فود
	حمله به متهم	اسنپ فود
اقدام تصحیحی	-	تپسی- اسنپ فود
تاسف	-	تپسی

همانگونه که از جدول بالا مشخص است شرکت تپسی از استراتژی های انکار(تغییر مقصر)، طفره رفتن از مسئولیت(نیت خوب)، کاهش آسیب (تعالی)، اقدام تصحیحی و ابراز تاسف استفاده کرده است، اما شرکت اسنپ فود فقط از دو استراتژی کاهش آسیب (تقویت، کوچک نمایی، تعالی و حمله به اتهام زننده) و اقدام تصحیحی استفاده کرده است.

عدم اطلاع‌رسانی به کاربران عادی

در اینستاگرام تپسی، اسنپ و اسنپ‌فود هیچ اشاره‌ای به هک نشده است (یا اگر شده، در همان زمان در حد استوری[1] بوده است که در صفحه باقی نمانده است). این موضوع نشان می‌دهد مدیران این پلتفرم‌ها اهمیتی به اطلاع‌رسانی به کاربران عادی در شبکه‌ی اجتماعی اینستاگرام که بیشترین استفاده توسط کاربران عادی را دارد نمی‌دهند. بدیهی است اطلاعیه‌ها در شبکه‌ی

[1] Story:
در اینستاگرام استوری‌ها بعد از ۲۴ ساعت از صفحه محو می‌شوند و بنابراین محتوای منتشره ممکن است استوری بوده باشد که پاک شده.

اجتماعی ایکس و یا وب‌سایت شرکت توسط عمده کاربران حتی مشاهده نمی‌شود و آنها ممکن است حتی متوجه نشوند هک اتفاق افتاده است. این عمل می‌تواند خود نوعی استراتژی انکار را نشان دهد زیرا عملا وقتی صفحه اینستاگرام این سرویس‌ها را مشاهده می‌کنیم هیچ بروز و ظهوری از هک اتفاق افتاده نمی‌بینیم. اسنپ در ایکس نیز به صفحه اسنپ‌فود اکتفا کرده و در صفحه خود اسنپ که در زمان نگارش این مقاله حدود ۳ برابر بیشتر دنبال‌کننده دارد محتوایی منتشر نکرده است. تپسی نیز در سایت خود محتوایی منتشر نکرده است.

اطلاع‌رسانی دیرهنگام

با بررسی خبرنگاران مشخص شده موضوع بحران هک تپسی حدود یک ماه قبل از اعلام بحران توسط بنیانگذار آن اتفاق افتاده بود. تپسی حدود یک ماه این مسئله را کتمان کرده بود پس از آن نیز تنها از طریق شبکه ایکس اطلاع‌رسانی را انجام داده بود. (مرزوقی، ۱۴۰۲) لذا امکان تاخیر و عدم اطلاع کاربران حتی پس از انتشار همچنان وجود داشت و درنتیجه مهم‌ترین اصل اطلاع‌رسانی که سرعت عمل است نادیده گرفته شده بود.

واکنش کاربران

در اینستاگرام کاربرانی که از هک مطلع شده بودند کامنت‌های مرتبط با هک را در پست‌های نامرتبط شرکت که به موضوعات دیگر مربوط بود منتشر می‌کردند. تعداد کامنت‌ها چندان زیاد نبود و هیچ پاسخی هم از سوی ادمین سرویس‌های آنلاین نداشت.

در ایکس کاربران برخورد متفاوتی داشتند. مخصوصا موضوع هک اسنپ‌فود به یکی از موضوعات ترند ایکس فارسی تبدیل شد و کاربران بسیاری به آن واکنش نشان دادند. از آنجا که گروه هکری نمونه‌ای شامل تعدادی از موارد هک شده منتشر کرده بود، بسیاری از توییت‌ها به شوخی کاربران با این نمونه‌ی منتشره اختصاص پیدا کرده بود.

همچنین با مطالعه توییت‌هایی که در پاسخ به اسنپ‌فود و تپسی منتشر شده بود، موارد زیر به دست آمد:

۱. توییت‌هایی که ناشی از نارضایتی از بیانیه بودند، در مورد اسنپ‌فود مکررا وجود داشتند. توییت‌هایی مانند: «نه عرضه نگهداری از اطلاعات مردم را دارید و نه شعور عذرخواهی بابت این اتفاق را، ذره‌ای همدلی، اندکی اظهار تاسف و مقادیری وعده (ولو سرخرمن) برای جلوگیری از اتفاقی مشابهه در این بیانیه نیست!» یا «عذرخواهی تو دهنتون کلا نمیچرخه؟» یا «خسته

نباشید، اینکه وظیفتونه اعلام نداره». اما در مورد تپسی کمتر دیده می‌شدند، و به مواردی مانند لحن توییت اشاره داشتند، مانند توییت زیر که در پاسخ به منشی‌پور نوشته شده بود:

«توییت فقط یه مدال افتخار کم داشت بندازین گردنتون . چرا انقد از عملکرد اشتباهتون راضی به نظر میاین؟!!!»

۲. در مورد اسنپ‌فود توییت‌هایی شامل توهین، طعنه و تمسخر مکررا دیده می‌شد اما در مورد تپسی تعداد این توییت‌ها کمتر بود. توییت‌های مشابه آنچه در ادامه آمده در پاسخ به اسنپ‌فود، در این دسته قرار داشتند: «خودتو ناراحت نکن پیش میاد»، «به به منت سرمون گذاشتید واقعا ممنون امیدواریم از پس جبران بر بیایم !!»، «گه بار اولته که داری هک میشی میتونی ۵۰ هزار تومن تخفیف بگیری ازشون».

۳. در هر دو مورد توییت‌هایی با موضوعاتی چون اشاره به لزوم شکایت، جریمه، دادگاه دیده می‌شد. مانند توییت فردی که در پاسخ به اسنپ‌فود گفته بود: «خاک بر سرتون، تقریبا هر جای دیگری از جهان بود از شما شکایت میشد و غرامت سنگینی باید پرداخت میکردین به کاربرا.» یا توییت فردی که در پاسخ به میلاد منشی‌پور گفته بود: «به عنوان کاربر قدیمی تپسی، میگم واقعا اگر راهی داشت که ازتون بابت این ناامنی اطلاعاتی شکایت کنم، صد در صد اینکارو انجام میدادم تا حداقل دو قرون دو زار از سودتون جهت افزایش امنیت اطلاعات کاربران هزینه میکردید.»

۴. در مورد تپسی واکنش‌های مثبت بیشتری دیده می‌شد، این واکنش در پاسخ به اسنپ‌فود کم تعداد بود. مثلا فردی در پاسخ به منشی‌پور گفته بود: «انقد تو ایران در این شرایط هیچ مسئولی عذرخواهی نمی‌کنه که ما الان به جای این‌که ناراحت باشیم، خوشحالیم :))))» یا فرد دیگری که نوشته بود: «ارادتم به شما و تپسی هزار برابر بیشتر شد.»

۵. در هر دو مورد غالب واکنش‌ها منفی است و نارضایتی از اطلاعیه، نارضایتی از اقدامات انجام شده بعد از هک، اشاره به مشکلات امنیتی، نارضایتی از عدم توجه کافی شرکت‌ها به باگ‌بانتی[1]، اشاره به عدم استفاده و تحریم اپلیکیشن و موارد مشابه را شامل می‌شود.

۶. در خصوص اسنپ‌فود عدم عذرخواهی در اطلاعیه مورد نارضایتی زیادی واقع شده، در خصوص تپسی عدم هزینه برای خرید اطلاعات از هکرها نارضایتی زیادی را برانگیخته است.

---

[1] Bug Bounty مسابقات کشف باگ و آسیب‌پذیری، برنامه‌هایی هستند که طی آن‌ها یک وب‌سایت یا اپلیکیشن .برای کشف رخنه‌ها و نقص‌های سرویس خود به افراد و هکرها پاداش و جایزه می‌دهد.

در نهایت به نظر می‌رسد ناتوانی شرکت‌ها در استفاده مناسب از استراتژی‌های ترمیم وجهه در ایجاد این واکنش‌های منفی بی‌تاثیر نباشد.

اقدامات گروه هکری

در پی هک تپسی گروه هکری در تلگرام خود اعلام کرد: «*فروش دیتا در پی بی‌مسئولیتی شرکت تپسی در حفظ اطلاعات مشتریان خود می‌باشد. این شرکت حاضر به پرداخت هیچ هزینه‌ای نشد و این بدین معناست که آنها برای اطلاعات شما کوچکترین اهمیتی قائل نیستند.*

جناب منشی‌پور ما به شما اخطار داده بودیم در صورتیکه مبلغ را پرداخت نکنید عواقب جبران ناپذیری برای شما دارد. بعد ۲ هفته مذاکره بی‌نتیجه با شما و پس از اینکه ما موضوع را عمومی کردیم، دیدید اوضاع خرابه ژست مسئولیت‌پذیری به خود گرفتید و توییت میزنید؟ خسته نشی یه وقت دلاور :) »(کانال تلگرام IRLeaks، ۱۴۰۲)

بدین ترتیب اولا مشخص شد تپسی قبل از اعلام عمومی از هک اطلاع داشته، و ثانیا اعلام شد که اطلاعات تپسی فروخته می‌شود.

بعد از هک اسنپ گروه هکری در تلگرام خود اعلام کرد: «*پیرو مذاکراتی که با تیم اسنپ‌فود داشتیم، دیتای این مجموعه به هیچکس فروخته نشده و نخواهد شد.*

تیم مدیریت اسنپ‌فود با رفتار حرفه‌ای نشان دادند اطلاعات مردم و آبروی برند براشون از هر چیزی ارزشمندتر است.»

تفاوت این دو پیام رسانه‌ای به حدی است که حتی این احتمال که کل این اتفاق پویشی[1] جهت ترویج[2] اسنپ باشد را بالا می‌برد. بحث درباره این موضوع از این مقاله خارج است، اما به هر حال اسنپ و تپسی اگرچه رویکردهای متفاوتی در کنترل بحران داشتند، از نظر نحوه اطلاع‌رسانی و پیام‌های منتشره بسیار مشابه عمل کردند.

بحث و نتیجه‌گیری

مطابق با نظریه بنت (۱۹۹۷) استراتژی‌ها مورد مطالعه قرار گرفت و مشخص شد استراتژی کاهش آسیب از نوع تعالی و استراتژی اقدام تصحیحی توسط هر دو شرکت مورد استفاده قرار گرفته است. تپسی از انکار از نوع تغییر مقصر، طفره رفتن از مسئولیت از نوع نیت خوب،

---

[1] Campaign
[2] promote

کاهش آسیبب از نوع تعالی، اقدام تصحیحی و تاسف استفاده کرده و اسنپ از کاهش آسیب از نوع تقویت، کاهش آسیب از نوع کمینه سازی، کاهش آسیب از نوع تعالی، کاهش آسیب از نوع حمله به متهم و اقدام تصحیحی استفاده کرده است. اگرچه در اینستاگرام انکار از نوع ساده انجام شده (با عدم واکنش نسبت به موضوع هک) اما در پیام‌های رسانه‌ای مطالعه شده از استراتژی‌های انکار از نوع انکار ساده، طفره رفتن از مسئولیت از نوع تحریک، ناتوانی و تصادف، و کاهش آسیب از نوع تمایز و جبران استفاده نشده است.

استراتژی‌ها توسط هر دو شرکت به صورت ناقص استفاده شده‌اند و احتمالا این موضوع با واکنش‌های منفی کاربران در ارتباط است. از آنجا که واکنش کاربران در سطح بالایی به شوخی و تمسخر گره خورده است، هر دو شرکت بحران را تا حد خوبی بدون پیامدهای بعدی پشت سر گذاشته‌اند و به نظر می‌رسد با توجه به نوع برخورد کاربران و شرکت، اگرچه استراتژی‌های ترمیم وجهه به خوبی استفاده نشده‌اند اما وجهه شرکت‌ها نیز مورد آسیب جدی نبوده است. هر دو شرکت بحران را پشت سر گذاشته و شرکت خود را توسعه داده‌اند، نسبت به قبل مشتریان بیشتری دارند و بدون یادآوری موضوع به حیات خود به خوبی ادامه داده‌اند. این موضوع البته ممکن است ناشی از فضای غیر رقابتی ایران باشد. در شرایطی که این دو شرکت عملا با رقیب دیگری مواجه نیستند، طبیعی است که حتی در صورت اشتباه در ترمیم وجهه، مشتری خود را از دست ندهند. این موضوع به مشتریان نیز مربوط است، وقتی بحران امنیت داده‌ها به سطح شوخی و تمسخر تقلیل یافته است، طبیعی است که مسئولین اطلاع‌رسانی نیز به بیانیه‌ی ساده‌ای اکتفا می‌کنند. مورد دیگر زمان اطلاع رسانی است. اگرچه که بنت می‌گوید بازسازی یک سازمان به طور عمده بستگی به این دارد که چقدر سریع به بحران پاسخ می‌دهد (Benoit, 1997) اما اولین واکنش از سوی تپسی یک ساعت و نیم بعد از انتشار این خبر در شبکه اجتماعی ایکس منتشر شد که بر اساس اعلام گروه هکری این اعلام زودهنگام نیز مدت‌ها بعد از اطلاع یافتن تپسی از هک منتشر شده است. اسنپ‌فود نیز حدود ۱۰ ساعت پس از انتشار این خبر بیانیه منتشر کرد و به هک شدنش واکنش نشان داد که به نظر می‌رسد هر دو پلتفرم سعی کرده‌اند پس از اعلام عمومی خبر هک شدنشان واکنش نشان دهند و تپسی موفق‌تر عمل کرده است. احتمالا این موضوع نیز در افزایش لایک توییت میلاد منشی‌پور نسبت به اسنپ‌فود موثر بوده است.

در مجموع، تحلیل نشان می‌دهد که هر دو شرکت با رویکردهای مشابه و کم‌اثر نتوانسته‌اند بحران را به طور کامل مدیریت کنند و اگر بحران به سرعت کنترل شده احتمالا ناشی از عدم حساسیت کاربرانی است که نسبت به داده‌های خود حساسیت ندارند، نمی‌توانند کاری از پیش ببرند و واکنش اصلی‌شان شوخی است و در یک فضای غیر رقابتی چاره‌ای غیر از استفاده از تپسی و اسنپ ندارند. البته استفاده از استراتژی‌های ناقص و تاخیر در اطلاع‌رسانی باعث واکنش‌های منفی کاربران لااقل در سطح مجازی شده است. هرچند برخی اقدامات تصحیحی و بهبود امنیت سایبری انجام شده، اما اقدامات انکار و عدم اطلاع‌رسانی در اینستاگرام، عملکرد شرکت‌ها در بحران را تحت تاثیر قرار داده است. این تحلیل نشان‌دهنده‌ی نیاز به تغییر و بهبود استراتژی‌های ارتباطات بحران و اطلاع‌رسانی در مواجهه با چنین وقایعی است. در نهایت می‌توان گفت شرکت‌ها و سازمان‌ها باید ضمن توجه بیشتر به ارتباطات بحران با لحاظ کردن زمینه‌های اجتماعی- فرهنگی جامعه ایران سعی در جلب نظر مشتریان و کاربران خود داشته باشند. به عبارت دیگر باید بر این امر واقف باشند که هزینه کردن برای ارتباطات بحران موثر و کارآمد می‌تواند بخشی از سرمایه‌گذاری آینده نگرانه این شرکت‌ها و سازمان‌ها باشد، چرا که هزینه برای بخش ارتباطات بحران می‌تواند در شرایط بحران مانع از آسیب جدی به وجهه و منافع آنها شود.

منابع

اجاق، زهرا(۱۴۰۱) شناسایی راهبردهای پاسخ به بحران همه گیری کووید ۱۹ در فضای رسانه ای ایران، فصلنامه ببرسی های مدیریت رسانه، دوره ۱، شماره ۴، صص ۴۴۳-۴۶۱

اسنپ (۱۴۰۲). گزارش عملکرد ۱۴۰۲. https://snapp.ir/1402-annual-report

بری هوپت، برینتی و آزودو، لورن(۱۴۰۲) برنامه ریزی ارتباطات بحران: راهبردهایی برای سازمان های غیر دولتی، ترجمه سیروان عبدی، تهران: نشرکارگزاران روابط عمومی.

غلامی، فرزاد و تقی‌زاده، مهراوه (۱۴۰۱) ارتباطات بحران و رسانه های محلی: چارچوب بندی اخبار سیل ۱۴۰۰در شبکه تلویزونی استانی کرمان، فصلنامه، جامعه، فرهنگ و رسانه، سال یازدهم شماره ۴۳، صص ۱۱-۴۱

کراندال، ویلیام ریک، پارنل، جان ای و اسپیلان، جان ایی(۱۳۹۶) مدیریت بحران: استراتژی های مدرن ایجاد تیم های مدیریت، قبل و بعد از بحران، ترجمه امید تشت زر، تهران: نشر گرایش تازه.

مرزوقی، زینب (۱۴۰۲). پاشنه‌آشیل هک بیگ‌دیتاها کجاست. فرهیختگان.

/https://farhikhtegandaily.com/page/241836

منشی‌پور، م. [MMonshipour]. (۱۱، شهریور، ۱۴۰۲). بازیابی شده از https://x.com/MMonshipour/status/1697967020896137515?t=YxJ7ygyNeJzMlDP1iUkWYA&s=19>

وبنا (۱۴۰۲) بررسی لایف‌وب از رفتار کاربران؛ اسنپ‌فود هک شد، کاربران توییت کردند و حتی خندیدند. https://webna.ir/39374/

وزیری، عباس (۱۴۰۲). اسنپ‌فود هک شد!. https://controladad.com/blog/khbr/snapp-food-hack/

Allison, R., Pegoraro, A., Frederick, E., & Thompson, A. J. (2020). When women athletes transgress: An exploratory study of image repair and social media response. Sport in Society, 23(6), 1023–1041. https://doi.org/10.1080/17430437.2019.1580266

Amoroso, D. L., & Chen, Y. A. N. (2017). Constructs Affecting Continuance intention in consumers with mobile financial apps: a dual factor approach. *Journal of Information Technology Management*, *28*(3), 1-24. http://jitm.ubalt.edu/XXVIII-3/article1.pdf

Benoit, W. L. (1997). Image repair discourse and crisis communication. Public Relations Review, 23(2), 177–186. https://doi.org/10.1016/ S0363-8111(97)90023-0 https://doi.org/10.1016/S0363-8111(97)90023-0

Benoit, W. L. (2015). Accounts, Excuses, and Apologies: Image Repair Theory and Research. United States: State University of New York Press. https://books.google.com/books/about/Accounts_Excuses_and_Apologies_Second_Ed.html?id=t1TVBAAAQBAJ

Bentley JM, Oostman KR, Shah SFA. (2018). We're Sorry But It's Not Our Fault: Organizational Apologies in Ambiguous Crisis Situations. Journal of Contingencies and Crisis Management 26(1): 138–149. https://doi.org/10.1111/1468-5973.12169

Bryant, J., Hopton, B., & Azodo, L. (2023). *Crisis communication planning: Strategies for non-governmental organizations* (S. Abdi, Trans.). Tehran: Public Relations Agents Publishing. (Original work published 2023). (in Persian)

Cheng, Y., & Cameron, G. (2018). The status of social-mediated crisis communication (SMCC) research: An analysis of published articles in 2002-2014. In L. Austin & Y. Jin (eds.), Social Media and Crisis Communication (pp. 9–20). Routledge. http://dx.doi.org/10.4324/9781315749068-2

Chiu, C. M., Chang, C. C., Cheng, H. L., & Fang, Y. H. (2009). Determinants of customer repurchase intention in online shopping. *Online Information Review*, *33*(4), 761-784. https://doi.org/10.1108/14684520910985710

Chon, M. G., & Kim, S. (2022). Dealing with the COVID-19 crisis: Theoretical application of social media analytics in government crisis management. Public Relations Review, 48(3), 102201. https://doi.org/10.1016/j.pubrev.2022.102201

Coombs, W. T. (2004). Impact of past crises on current crisis communication: Insights from situational crisis communication theory. Journal of Business Communication, 41(3), 265–289. https://doi.org/10.1177/0021943604265607

Coombs, W. T., Sherry J. Holladay. (2010). The Handbook of Crisis Communication (Handbooks in Communication and Media. Wiley-Blackwell. https://doi.org/10.1002/9781444314885

Crandall, W. R., Parnell, J. A., & Spillan, J. E. (2017). *Crisis management: Modern strategies for building management teams before and after crises* (O. Tashtazar, Trans.). Tehran:

Geraresh-e Tazeh Publishing. (Original work published 2017) (in Persian). https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449

Frandsen, F., Johansen, W. (2016). Organizational Crisis Communication: A Multivocal Approach. United Kingdom: SAGE Publications. https://www.researchgate.net/publication/305943066_Organizational_Crisis_Communiication_A_Multivocal_Approach

Gholami, F., & Taghizadeh, M. (2022). *Crisis communication and local media: Framing news coverage of the 2021 floods in Kerman provincial television network*. Journal of Society, Culture and Media, 11 (43), 11-41. (in Persian) https://www.jscm.ir/article_158627.html

Gilpin, D. R., & Murphy, P. J. (2008). *Crisis management in a complex world*. Oxford University Press. https://academic.oup.com/book/10743

Howard, J. M. (2020). Trains, Twitter and the social licence to operate: An analysis of Twitter use by train operating companies in the United Kingdom. Case Studies on Transport Policy, 8(3), 812–821. http://dx.doi.org/10.1016/j.cstp.2020.06.002

Kamboh, S. A., Ittefaq, M., & Jin, Y. (2024). Crisis communication for public organizations: Examining Pakistan Railways' use of information technology and social media for image repair. *Journal of Contingencies and Crisis Management*, 32, e12496. https://doi.org/10.1111/1468-5973.12496

Knight, Richard & Nurse, Jason R. C. (2020). A framework for effective corporate communication after cyber security incidents. Computers & Security ،99 ،102036.. https://doi.org/https://doi.org/10.1016/j.cose.2020.102036

Kuipers, Sanneke & Schonheit, Michael. (2021). Data Breaches and Effective Crisis Communication: A Comparative Analysis of Corporate Reputational Crises. Corporate Reputation Review. http://dx.doi.org/10.1057/s41299-021-00121-9

L. Heath, Robert & O'Hair, H. Dan. (2010) Handbook of Risk and Crisis Communication. United Kingdom: Taylor & Francis.

Marzouqi, Z. (2023). *Where is the Achilles' heel of big data hacking?* Farheekhtegan, https://doi.org/10.4324/9781003070726

Monshipour, M. [@MMonshipour]. (2023, September 2). *[Tweet content in Persian]*. Twitter. Retrieved from <URL> https://x.com/MMonshipour/status/1697967020896137515?t=YxJ7ygyNeJzMlDP1iUkWYA&s=19<

Ojagh, Seyedeh Zahra (2022). Identifying crisis response strategies during the Covid-19 pandemic in the sphere of Iranian Media. Media Management Review, 1(4), 399-417. (in Persian) doi: https://doi.org/10.22059/MMR.2023.355032.1040

Olaniran, Bolanle & Potter, Andrew & Ross, Katy & Johnson, Brad. (2014). A Gamer's Nightmare: An Analysis of the Sony PlayStation Hacking Crisis. Journal of Risk Analysis and Crisis Response. 4. 151. 10.2991/jrarc.2014.4.3.4 . https://doi.org/10.2991/jrarc.2014.4.3.4

Park, Hanna. 2017. Exploring Effective Crisis Response Strategies. Public Relations Review. https://doi.org/10.1016/j.pubrev.2016.12.001.

Ruohonen, J., Hjerppe, K., & Kortesuo, K. (2024). Crisis Communication in the Face of Data Breaches. *arXiv preprint arXiv:2406.01744*. https://doi.org/10.48550/arXiv.2406.01744

Sellnow, T.L. & Seeger, M.W. (2013). Theorizing Crisis Communication. Wiley. https://books.google.com/books/about/Theorizing_Crisis_Communication.html?id=YGUQEAAAQBAJ

Spradley, R. Tyler. (2017). Crisis Communication in Organizations. In The International Encyclopedia of Organizational Communication. https://doi.org/10.1002/9781118955567.wbieoc050

Upadhyay, S., & Upadhyay, N. (2023). Mapping crisis communication in the communication research: what we know and what we don't know. *Humanities and Social Sciences Communications*, *10*(1), 1-19

Vaziri, A. (2023). *Snappfood was hacked!* [Article]. https://controladad.com/blog/khbr/snapp-food-hack

Webna. (2023). *LifeWeb analysis of user behavior: Snappfood was hacked, users tweeted and even laughed*. [Online news article]. Retrieved from <URL>https://webna.ir/39374/

Zhang, J., & Benoit, W. L. (2004). Message strategies of Saudi Arabia's image restoration campaign after 9/11. Public Relations Review, 30(2), 161–167. https://doi.org/10.1016/J.PUBREV.2004.02.006