Changes in Users' Attitudes to Security Breaches: A Study of T-Mobile Breaches

(Short Paper)

Yoongi Kim
Ramakrishna Ayyagari
University of Massachusetts Boston
r.ayyagari@umb.edu

Abstract

The technological advances in mobile devices have been causing security issues. Mobile devices are becoming popular targets because of advances in almost PC-like capabilities. Installing malicious code on mobile devices can seriously compromise users' data. Despite the continuous efforts to prevent security breaches, cyber-attacks and breaches are increasing. T-Mobile, a wireless service provider with over 100 million customers in the states, is a prime example. Since 2021, T-Mobile has been experiencing numerous security breaches. This research follows the security breaches that affected T-Mobile subscribers since 2021, which resulted in personal data leaks of over 76 million subscribers. We investigate the responses of T-Mobile users on Reddit to the series of breaches over the years. Based on the investigation, we aim to discover how users' perceptions change over time in response to multiple breaches.

Introduction

As mobile device usage continues to grow in people's everyday lives, the danger of security incidents continues to grow simultaneously. Security breaches portray a significant risk to both firms and users since they involve unauthorized access to data and personally identifiable information executed by a wide range of methods (e.g., hacking, phishing, smishing, etc.) (Culnan & Williams, 2009). Mobile devices such as laptops and smartphones let employees access data from anywhere. Smartphones are quickly becoming primary targets for cyber-attacks since the hardware and operating systems are becoming just as capable as computers. Naturally, the security standards required in computers are enforced in smartphone usage (Delac et al., 2011). Firms try to minimize incidents and protect sensitive data. Firms deal with employee-owned devices to a certain degree, but newer threats continue to emerge to raise challenges (McLaughlin & Gogan, 2018).

The number of security breaches threatening user privacy is rising as mobile devices carrying sensitive information are increasing to fulfill users' constantly growing craving for social connections. This vastly improved connectivity and increasing social media usage are transforming the digital environment, leading to vast amounts of data that could potentially be compromised. User data becomes easily obtainable and valuable but vulnerable simultaneously (Labrecque, 2021). With a successful attack on a smartphone, attackers can access the camera, microphone, and GPS data and even snatch SMS messages, which are severe threats to users' privacy (Delac et al., 2011). For example, mobile payment applications that have become common in many countries due to their convenience may face severe threats from the attacks. Apple, Google, Samsung, PayPal, and other companies developed their mobile payment

platforms. Most companies use multi-factor authentication to verify users via SMS messages (Wang et al., 2016). Intercepting SMS messages could make multi-factor authentication useless.

Protecting users' data is an essential task for firms and end users. However, the motivation to accomplish the task may be diminishing over time as users become numb to the constant security breaches that happen every day. Therefore, we study users' behavioral change over time regarding the effort to push firms to put more effort into protecting their data.

Background

Since 2021, T-Mobile has suffered colossal data breaches, including losing personally identifiable information (Corkery, 2022). Approximately 76 million subscribers had their data exposed to cyberattacks, including SSNs, phone numbers, and addresses. Thus far, the company has experienced one of the most severe data breaches in US history. Therefore, we use T-Mobile breaches as our study space and analyze T-Mobile subscribers' reactions to repeated data breach incidents.

Theoretical Framework

We use Situation awareness as a potential framework to understand users' perceptions to repeated breaches. Situation awareness is acknowledging what is happening around us. Acknowledging incidents, such as data breaches, causes emotional changes, which lead to various responses. Endsley (1988) provides directions with situation awareness theory to explore the responses. We categorize the responses into three situation awareness stages -perception, comprehension, and projection. Perception is the fundamental state that lets us identify emotions, such as anxiety or fear. A fundamental perception of information helps form the correct picture of the situation. Then, the comprehension stage is where people interpret and store the information to get past the perception stage. Lastly, projection represents the highest level of situational understanding. Affected users in this stage expect some resolutions. We anticipate that the stages show differences among users due to repeated incidents over the years.

Study Design

We collect data from the T-Mobile subreddit on Reddit. Reddit consists of interest-based communities (subreddits), which are made of content shared by users. Users express their interests by joining the subreddits. Users communicate with other users via posting content or comments. Reddit prioritizes content primarily based on popularity displayed by upvotes and downvotes. Users may filter and block content, but all users in the same subreddit see the same content (Jürgens & Stark, 2017). Using Reddit in research has been gaining popularity recently. For instance, Kitchens et al. (2020) used Reddit data to identify different impacts on news consumption by platform. Li et al. (2022) utilized Reddit users' responses to discover the characteristics of collective trolling in virtual communities.

The data from the T-Mobile subreddit includes users' reactions to the posts regarding data breaches since 2021. Specifically, we collect the number of upvotes, the number of comments, and the content of the comments. The data will provide an opportunity to understand the users' reaction changes to those incidents over time and a foundation for future research to study users' motivation to protect their data.

References

Corkery, M. (2022, July 22). T-Mobile Reaches $500 Million Settlement in Huge 2021 Data Breach. Retrieved from The New York Times: https://www.nytimes.com/2022/07/22/business/t-mobile-hacking-settlement.html

Culnan, M. J., & Williams, C. C. (2009). How ethics can enhance organizational privacy: Lessons from the Choicepoint and TJX data breaches. MIS Quarterly, 33(4), 673-687.

Delac, G., Silic, M., & Krolo, J. (2011, May). Emerging security threats for mobile platforms. In 2011 Proceedings of the 34th International Convention MIPRO (pp. 1468-1473). IEEE.

Endsley, M. R. (1988, October). Design and evaluation for situation awareness enhancement. In Proceedings of the Human Factors Society annual meeting (Vol. 32, No. 2, pp. 97-101). Sage CA: Los Angeles, CA: Sage Publications.

Jürgens, P., & Stark, B. (2017). The power of default on Reddit: A general model to measure the influence of information intermediaries. Policy & Internet, 9(4), 395-419.

Kitchens, B., Johnson, S. L., & Gray, P. (2020). Understanding Echo Chambers and Filter Bubbles: The Impact of Social Media on Diversification and Partisan Shifts in News Consumption. MIS quarterly, 44(4).

Labrecque, L. I., Markos, E., Swani, K., & Peña, P. (2021). When data security goes wrong: Examining the impact of stress, social contract violation, and data type on consumer coping responses following a data breach. Journal of Business Research, 135, 559-571.

Li, Y. J., Cheung, C. M., Shen, X. L., & Lee, M. K. (2022). When socialization goes wrong: Understanding the we-intention to participate in collective trolling in virtual communities. Journal of the Association for Information Systems, 23(3), 678-706.

McLaughlin, M. D., & Gogan, J. (2018). Challenges and best practices in information security management. MIS Quarterly Executive, 17(3), 12.

Wang, Y., Hahn, C., & Sutrave, K. (2016, February). Mobile payment security, threats, and challenges. In 2016 second international conference on mobile and secure services (MobiSecServ) (pp. 1-5). IEEE.