DOI: https://doi.org/10.48009/3_iis_2022_121

Social media privacy and security concerns: Trust and awareness

Alex Koohang, *Middle Georgia State University, USA, alex.koohang@mga.edu*
Jeretta Horn Nord, *Oklahoma State University, USA, jeretta.nord@okstate.edu*
Kevin Floyd, *Middle Georgia State University, USA, kevin.floyd@mga.edu*
Joanna Paliszkiewicz, *Warsaw University of Life Sciences, Poland, joanna_paliszkiewicz@sggw.edu.pl*

Abstract

This study sought to build two prediction models to find out 1) which predictor variables, i.e., social media privacy concerns and social media security concerns are most influential in predicting social media user *trust* and 2) which predictor variables, i.e., social media privacy concerns and social media security concerns are most influential in predicting social media user *awareness*. An instrument with four constructs was used to collect data from college students who were studying in the field of information technology. Collected data were analyzed through multiple regression analyses. Results for the first model indicated that both predictor variables were significant in predicting social media user trust, with privacy concerns being the most influential predictor variable followed by social media security concerns. Results for the second model indicated that both predictor variables were significant in predicting social media user awareness, with privacy concerns being the most influential predictor variable followed by social media security concerns. These findings are discussed, and recommendations are made for both practice and future research.

Keywords: Social media, privacy concerns, security concerns, trust, awareness

Introduction

Social media usage growth has not slowed down in 2022. Datareportal (2022) reports that as of April 2022, there were 4.65 billion social media users around the world, equating to nearly 59% of the total global population and 75% of the eligible global population. Nearly 9 out of 10 Internet users use social media each month and the average growth is more than 10 new users every second. A typical social media user actively uses or visits an average of 7.4 different social platforms each month and spends an average of close to 2½ hours per day using social media. Facebook, YouTube, WhatsApp, Instagram, WeChat, TikTok, and Facebook Messenger were among the top social media platforms respectively (Datareportal, 2022). With the constant increase in social media usage, social media privacy and security challenges become even more imperative as users become concerned about their privacy and security on social media platforms. Furthermore, users' privacy and security concerns may be associated with users' trust and users' awareness of threats and risks on social media platforms.

The purpose of this study is to create two prediction models. The first model includes two predictor variables and one dependent variable. The predictor variables are social media privacy concerns and social media security concerns. The dependent variable is social media trust. The second model consists of two predictor variables and one dependent variable. The predictor variables are social media privacy concerns and social media security concerns. The dependent variable is social media awareness.

For each prediction model, we will seek to find out which of the predictor variables are most influential in predicting the dependent variable. These variables are adopted from a study conducted by Koohang et al. (2021, p. 134) and their definitions are as follows.

Social media privacy concerns are defined as "… the collection of personal information, secondary usage of personal information, improper access of personal information, and lack of control of personal information." *Social media security concerns* are defined as "… identity theft (attackers stealing personal information); impersonation/social phishing (attackers impersonating a real person through a fake website to steal data, login credentials, credit card numbers, etc.); hijacking (attackers taking control over one's profile); image retrieval/analysis (attackers using face and image recognition software to find more information about users and their linked profiles); and malware attacks (attacker sending malware injected scripts or malicious software to perform activities on users' device without their knowledge)." *Social media user trust* is defined as "… integrity trust (where social media platforms are trustworthy to protect users' privacy and security); benevolence trust (where social media platforms keep users' best interests and well-being in mind); and competence trust (where social media platforms are perceived to be competent in protecting and safeguarding users' personal information)." *Social media use awareness* is defined as "… users being aware of potential threats and risks on social media platforms associated with their security and privacy that result in possible negative consequences, harm, and or loss." (Koohang et al., 2021, p. 134)

Consistent with the purpose of this study, we ask two questions.

1) Which of the two predictor variables (i.e., social media privacy concerns and social media security concerns) are most influential in predicting social media user trust?

2) Which of the two predictor variables (i.e., social media privacy concerns and social media security concerns) are most influential in predicting social media user awareness?

Review of the literature

Social media privacy and security concerns

Privacy concerns have received considerable attention since the increased collection of personal information online and the development of online technologies (Young, Quan-Haase, 2013). For example, privacy concerns are the lack of control of one's personal information (Smith et al., 2011; Stone et al., 1983; Clarke 1998); including the general concerns that reflect individuals' fears about the possible loss of privacy (Malhotra et al., 2004). Hong and Thong (2013, p. 276) described privacy concerns as "… the degree to which an Internet user is concerned about website practices related to the collection and use of his or her personal information." Benisch et al. (2011) reported privacy on social media sites as a major concern for users.

Literature has documented numerous studies about privacy concerns on social media, i.e., social media privacy concerns about trusting beliefs and risk beliefs (Koohang et al., 2018); addressing data privacy concerns when using social media (Di Minin et al., 2021); impact of privacy concerns on social media (Bright et al., 2021; Ming, 2021); consumers' concerns about their personal information on social media (Bright et al., 2022); and concerns about collection and control of personal information (Cain & Imre, 2021). Wang et al. (2019) aimed to facilitate an understanding of how to mitigate the privacy concerns of social media users who have experienced privacy invasion. Ozdemir et al. (2017) studied antecedents and outcomes of information privacy concerns in a peer context on social media.

Norton (n.d.) lists eleven ongoing social media serious threats and scams that can harm users. They are likejacking/clickjacking, fake giveaways, unbelievable news that is malware, affiliate scams, fake friends or followers, phishing attempts with fake links, catfishing/dating scams, cyberbullying, identity theft, fake apps loaded with viruses or real apps that will sell your data, and private messages with dodgy links.

Jain et al. (2021) stated that social network security threats can be put into three categories, i.e., conventional, modern, and targeted. Conventional threats include spam malware, phishing, and identity theft. Modern threats are attacks that use advanced techniques to compromise accounts of users such as clickjacking, hijacking, deanonymization, inference attack, profile cloning, cyber espionage, and cross-site scripting. Targeted attacks are pointed at particular users, and they include cyber-grooming and cyber-stalking.

With the increasing number of social network users, the information shared in social networks spreads very fast, making it attractive for attackers to gain information (Fox & Royne, 2018). Forbes (2022) reported that online security threats are becoming increasingly serious. The top security threats of 2022 as reported by Forbes are credential reuse attacks, insider threats, man-in-the-middle attacks, phishing, ransomware, watering hole attack, spyware, social engineering attack, DDoS attack, and cloud crypto mining.

Social media user trust and awareness

Trust is essential in assessing the quality and credibility of information and determining how information flows through the network (Adali et al., 2010). Rotter and Stein (1971) defined trust as an expectancy that the promise of an individual or a group can be relied upon. Rousseau et al. (1998) described social trust as the willingness to accept the vulnerability to the actions of others based on positive expectations regarding others' intentions and/or behavior. Corritore et al. (2003) stated that trust is the expectation that a user's vulnerabilities would not be misused and manipulated in an online setting.

Zhou (2020) examined the effect of information privacy concerns on users' social shopping intention. Based on the 340 responses, the author indicated that while disposition to privacy positively affects privacy concerns, both reputation and laws negatively affect privacy concerns, which in turn decreases social shopping intention. In addition, trust partially mediates the effect of privacy concerns on social shopping intention. According to Paramarta et al. (2018), social media users with control over their information flow and privacy protection for their profiles are more likely to trust social media sites. According to Dhami et al. (2013), users' ability to trust social media depends on their belief that their personal information is secure, protected, and in their control.

D'Arcy et al. (2009) asserted that awareness promotes openness among employees. Koohang et al. (2021) believed that awareness is imperative in safeguarding social media users against risks and threats. Shaw et al. (2009, p. 92) stated that security awareness is "… the degree of understanding of users about the importance of information security and their responsibilities and acts to exercise sufficient levels of information security control." Furthermore, Bulgurcu, Cavusoglu, and Benbasat (2010) defined security awareness as "… an employee's overall knowledge and understanding of potential issues related to information security and their ramifications" (p. 532). Yerby, et al. (2019) concluded that awareness of social media was a significant factor in avoiding identity theft and securing users' personal information. The authors further stated that increased awareness of threats contributes to users' behavior modification to protect their personal information against threats on social media sites (Yerby et al., 2019).

Methodology

Instrument

The instrument for this study was designed by Koohang et al. (2021). It consisted of four constructs, each construct with its associated items. The constructs were social media privacy concerns, social media security concerns, social media user trust, and social media user awareness. The instrument, via factor analysis, concluded that all four constructs had retained all their designated items, indicating that each construct was empirically validated to be reliable and interpretable among all its associated items. The constructs with their associated items are as follows.

"Privacy Concerns Construct (Defines collection, secondary usage, improper access, and control)

1. I am concerned that social media sites are collecting my personal information.
2. I am concerned that social media sites share/sell my stored personal information in their databases to other companies.
3. I am concerned that social media sites do not devote enough time and effort to preventing unauthorized access to my personal information.
4. It bothers me when I do not have control or autonomy over decisions about how my personal information is collected, used, and shared by social media sites.

Security Concerns Construct (Defines identity theft, impersonation / social phishing, hijacking, image retrieval and analysis, and malware attacks**)**

When I am on social media sites, I am concerned about
1. Identity theft (attacker stealing my personal information).
2. Impersonation/Social phishing (attacker impersonating a real person through a fake website to steal my data, including login credentials and credit card numbers, etc.).
3. Hijacking (attacker taking control over my profile).
4. Image retrieval and analysis (attacker using face and image recognition software to find more information about me and my linked profiles).
5. Malware attacks (attacker sending malware injected scripts or malicious software to perform activities on my device without my knowledge).

Trust Construct (Defines integrity trust, benevolence trust, and competence trust)

When it comes to privacy and security, the social media sites I belong to:
1. are trustworthy.
2. keep my best interests and well-being in mind.
3. are competent in protecting and safeguarding my personal information.

Awareness Construct (Defines security threats/risks, privacy threats/risks, and harm/loss)

When using social media sites
1. I am aware of the potential security threats and risks and their negative consequences.
2. I am aware of potential privacy threats and risks and their negative consequences
3. I am aware that there is potential for harm/loss associated with my security and privacy." (Koohang et al., 2021, pp. 136-137)

The response scales for all items of the instrument were 7 = completely agree, 6 = mostly agree, 5 = somewhat agree, 4 = neither agree nor disagree, 3 = somewhat disagree, 2 = mostly disagree, 1 = completely disagree.

Subjects and procedure

We used SurveyMonkey™, an Internet survey company to administer the instrument to approximately 1000 undergraduate and graduate students who were studying in various fields of information technology such as cybersecurity, forensics, web development, networking administration, software engineering, and data analytics. This survey was approved, before administering, by the Institutional Research Board of the university where this study took place. At the time of this study, we had received 319 surveys. Of the 319, we eliminated three incomplete surveys. This yielded a total of 316 completed surveys that were used for data analysis. The subjects were males (N = 168) and females (N = 148). The subjects' age groups were 18 - 20 (N = 118), 21 - 29 (N = 110), 30 – 39 (N = 40), and 40 or older (N = 48). The most popular social media used by subjects were Facebook, Instagram, Twitter, Snapchat, Pinterest, and LinkedIn. The subjects were 18 years and older. They were assured confidentiality and anonymity.

Data analysis

To answer the research questions, we used two separate multiple regression analyses (the Enter method) – one for each prediction model. For the first model, we sought to determine the predictor variables (i.e., social media privacy concerns and social media security concerns) that are most influential in predicting social media user trust. For the second model, we sought to determine predictor variables (i.e., social media privacy concerns and social media security concerns) that are most influential in predicting social media user awareness. Stevens (2012) stated that the coefficients table in multiple regression analysis determines the predictor variables that are influential in predicting the dependent variable. Before any interpretation of the results in the coefficients table, the following tests are performed.

1) The multicollinearity test – the results must indicate the non-existence of multicollinearity. The non-existence of multicollinearity is indicated by the tolerance level where the values of all predictor variables must be above .1 and the variance inflation factor (VIF) where the values of all predictor variables should not be greater than 10.

2) The model summary/goodness of fit test points to how well the predictor variables predict the dependent variable. It includes multiple correlations (R), squared multiple correlations - coefficient of determination (R^2), or "goodness of the fit" with a value between 0.0 (failing to accurately model the data) to 1.0 (highly reliable prediction model), and adjusted squared multiple correlations (R^2adj).

3) The ANOVA test should indicate a linear relationship between the dependent variable and the predictor variables. To achieve this, the F test must be significant (p-value should be equal to or less than .05).

Results

Research question 1: Which of the two predictor variables (i.e., social media privacy concerns and social media security concerns) are most influential in predicting social media user trust?

The results indicated the non-existence of multicollinearity. The tolerance level for both predictor variables was above .1 (social media privacy concerns = .634 and social media security concerns = .634) and the VIF for both predictor variables indicated a value less than 10 (social media privacy concerns = 1.577 and social media security concerns = 1.577).

The model summary results were R = .344, R^2 = .118, R^{2}adj = .112, and standard error of the estimate = 1.455. The R^2 in the model summary suggests that 11% of the dependent variable (social media user trust) is predicted by the independent variables (social media privacy concerns and social media security concerns) indicating a reliable prediction model. The ANOVA test (F = 20.937 and p <.001) indicated a linear relationship between the dependent variable (social media user trust) and the predictor variables (social media privacy concerns and social media security concerns).

Table 1 shows the coefficients. As can be seen, both predictor variables contributed significantly to the prediction model. The most influential predictor variable was social media privacy concerns (β = -.413, p < .001) followed by social media security concerns (β = .150, p = .025). The β value for social media privacy concerns was negative indicating that the dependent variable of social media user trust decreased in response to an increase in social media privacy concerns. Conversely, the β value for social media security concerns was positive indicating that the dependent variable of social media user trust increased in response to greater social media security concerns. Tables 2 and 3 show the descriptive statistics and correlations.

Table 1: Coefficients results

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	5.391	.416		12.959	**<.001**
	Privacy	-.531	.086	-.413	-6.193	**<.001**
	Security	.163	.072	.150	2.253	**.025**

Dependent variable: Social media user trust

Table 2: Descriptive Statistics

	Mean	Std. Deviation	N
Trust	3.1308	1.54524	316
Privacy	5.8679	1.20125	316
Security	5.2671	1.42657	316

Table 3: Correlations

		Trust	Privacy	Security
Trust	Pearson Correlation	1	-.322**	-.100
	Sig. (2-tailed)		<.001	.077
	N	316	316	316
Privacy	Pearson Correlation	-.322**	1	.605**
	Sig. (2-tailed)	<.001		<.001
	N	316	316	316
Security	Pearson Correlation	-.100	.605**	1
	Sig. (2-tailed)	.077	<.001	
	N	316	316	316

**. Correlation is significant at the 0.01 level (2-tailed).

Research question 2: Which of the two predictor variables (i.e., social media privacy concerns and social media security concerns) are most influential in predicting social media user awareness?

The results indicated the non-existence of multicollinearity. The tolerance level for both predictor variables was above .1 (social media privacy concerns = .634 and social media security concerns = .634) and the VIF for both predictor variables indicated a value less than 10 (social media privacy concerns = 1.577 and social media security concerns = 1.577). The model summary results were R = .368, R^2 = .135, R^2adj = .130, and standard error of the estimate = .839. The R^2 in the model summary suggests that 13% of the dependent variable (social media user awareness) is predicted by the independent variables (social media privacy concerns and social media security concerns) indicating a reliable prediction model. The ANOVA test (F = 24.511 and p <.001) indicated a linear relationship between the dependent variable (social media user awareness) and the predictor variables (social media privacy concerns and social media security concerns).

Table 4 shows the coefficients. As can be seen, both predictor variables contributed significantly to the prediction model. The most influential predictor variable was social media privacy concerns (β = .270, p < .001) followed by social media security concerns (β = .136, p = .041). The positive β value for both social media privacy concerns and social media security concerns indicated that the dependent variable of social media user awareness increased in response to greater social media privacy concerns and social media security concerns. Tables 5 and 6 show the descriptive statistics and correlations.

Table 4: Coefficients

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	4.523	.240		18.846	<.001
	Privacy	.202	.049	.270	4.085	<.001
	Security	.086	.042	.136	2.056	.041

Dependent Variable: Social media user awareness

Table 5: Descriptive Statistics

	Mean	Std. Deviation	N
Awareness	6.1603	.90050	316
Privacy	5.8679	1.20125	316
Security	5.2671	1.42657	316

Table 6: Correlations

		Awareness	Privacy	Security
Awareness	Pearson Correlation	1	.352**	.299**
	Sig. (2-tailed)		<.001	<.001
	N	316	316	316
Privacy	Pearson Correlation	.352**	1	.605**
	Sig. (2-tailed)	<.001		<.001
	N	316	316	316
Security	Pearson Correlation	.299**	.605**	1
	Sig. (2-tailed)	<.001	<.001	
	N	316	316	316

**. Correlation is significant at the 0.01 level (2-tailed).

Discussion

Two separate multiple regression models (prediction models) were created. The first model included two predictor variables (i.e., social media privacy concerns and social media security concerns) and one dependent variable (i.e., social media user trust). We then sought to determine which predictor variables were most influential in predicting social media user trust. The second model included two predictor variables (i.e., social media privacy concerns and social media security concerns) and one dependent variable (i.e., social media user awareness). We then sought to determine which predictor variables were most influential in predicting social media user awareness.

The findings for the first model revealed that both predictor variables contributed significantly to the prediction model. However, the most influential predictor variable was social media privacy concerns followed by social media security concerns. The β value for social media privacy concerns was negative indicating that social media user trust decreased in response to an increase in social media privacy concerns. Conversely, the β value for social media security concerns was positive indicating that social media user trust increased in response to greater social media security concerns. These findings imply that an increase in users' social media privacy concerns that included collection, secondary usage, improper access, and control of personal information by social media sites decreased users' social media trust. On the other hand, the increase in users' social media security concerns which included identity theft, impersonation/social phishing, hijacking, image retrieval/analysis, and malware attacks increased users' social media trust. This finding is interesting because one may expect that an increase in users' social media security concerns would have decreased users' social media trust. It is noteworthy to mention that the subjects of this study were information technology students with skills in security and other IT topics.

Could the subjects' confidence in understanding and mitigating security threats, in general, contribute to this finding? After all, social media sites are responsible for the collection, secondary usage, improper access, and control of personal information. However, safeguarding against identity theft, impersonation/social phishing, hijacking, image retrieval/analysis, and malware attacks are typically the responsibility of individuals.

The findings for the second model revealed that both predictor variables contributed significantly to the prediction model. The most influential predictor variable was social media privacy concerns followed by social media security concerns. The positive β values for both social media privacy concerns and social media security concerns indicate that social media user awareness increased in response to greater social media privacy concerns and social media security concerns. These findings imply that an increase in concerns about social media privacy and security increases social media user awareness. Being aware of the potential privacy and security threats and risks and their negative consequences that can cause potential harm/loss is a good thing, however, being merely aware of these issues will not safeguard users and their organizations against security and privacy threats and risks. Brain (2021) reported that 98% of employees have social media for personal use, 80% of workers use social media on the job, and 50% of employees post information about their company online. Furthermore, "employees' social media content reaches 561% further than official company channels and receives 800% more engagement." Given these statistics, organizations should take social media awareness and training seriously to protect their assets. Wilson and Hash (2003, p. 7) stated that "… awareness and training should be focused on the organization's entire user population. Management should set the example for proper IT security behavior within an organization. An awareness program should begin with an effort that can be deployed and implemented in various ways and is aimed at all levels of the organization including senior and executive managers."

To safeguard users and organizations against privacy and security threats and risks, we recommend that organizations make social media awareness and training programs a top strategic priority. Social media awareness training and programs should be considered regular and routine for any organization. A social media awareness and training program should include privacy and security topics that embrace and enforce privacy issues to protect personal information and security issues to protect organizations' assets. For example, privacy topics as described by Johnsen (2022) should include enforcing users to read the social media site's terms to see what information (especially private information) they are agreeing to share; being able to understand and adjust privacy settings on social media; knowing what types of personal data social media sites collect, store, and share; and carefully considering what personal details the user provides in their profile. Topics for social media security awareness and training should include identity theft, impersonation/social phishing, hijacking, image retrieval and analysis, and malware attacks. These topics should include examples and exercises/drills to make sure users understand to avoid becoming victims of threats.

This study is not without limitations. First, our sample included college students who were studying in the field of information technology with major concentrations such as cybersecurity, forensics, web development, networking administration, software engineering, and data analytics. To improve the generalizability of results, future studies should be carried out to include samples from other fields of study. Second, the sample of convenience used in this study may be substituted by a random sample in future studies to possibly enhance the generalizability of the results. Third, this study used a self-reported survey instrument to collect data, although this method is commonly used in research design, it may have the potential for bias that could influence the generalizability of the results. Future studies may consider a scenario-based instrument that could improve the generalizability of the results. In addition to the variables used in this study, future research may be carried out to include other dependent variables, i.e.., behavioral variables, that impact social media privacy and security concerns.

References

Dhami, A., Agarwal, N., Chakraborty, T. K., Singh, B. P., & Minj, J. (2013, February). Impact of trust, security and privacy concerns in social networking: An exploratory study to understand the pattern of information revelation in Facebook. In *2013 3rd IEEE International Advance Computing Conference (IACC)* (pp. 465-469). IEEE.

Adali, S., Escriva, R., Goldberg, M. K., Hayvanovych, M., Magdon-Ismail, M., Szymanski, B. K., Wallace, W.A. & Williams, G. (2010). *Measuring behavioral trust in social networks*. 2010 IEEE International Conference on Intelligence and Security Informatics, pp. 150-152. available at: https://doi.org/10.1109/ISI.2010.5484757

Benisch, M., Kelley, P. G., Sadeh, N., & Cranor, L. F. (2011). Capturing location-privacy preferences: quantifying accuracy and user-burden tradeoffs. *Personal and Ubiquitous Computing*, *15*(7), 679-694.

Brain, J. (2021). *Social Media in the Workplace: What Every Executive Should Know*. Retrieved from https://everyonesocial.com/blog/social-media-in-the-workplace/

Bright, L. F., Lim, H. S., & Logan, K. (2021). "Should I Post or Ghost?": Examining how privacy concerns impact social media engagement in US consumers. *Psychology & Marketing*, *38*(10), 1712-1722.

Bright, L. F., Logan, K., & Lim, H. S. (2022). Social Media Fatigue and Privacy: An Exploration of Antecedents to Consumers' Concerns regarding the Security of Their Personal Information on Social Media Platforms. *Journal of Interactive Advertising*, 1-16.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, *34*(3), 523-548.

Cain, J. A., & Imre, I. (2021). Everybody wants some: Collection and control of personal information, privacy concerns, and social media use. *New Media & Society*, https://doi.org/10.1177/14614448211000327

Clarke, R. A. (1998). Information technology and dataveillance. *Communications of the ACM, 31*(5), 498–512.

Corritore, C. L., Kracher, B., & Wiedenbeck, S. (2003). On-line trust: concepts, evolving themes, a model. *International Journal of Human-Computer Studies*, *58*(6), 737-758.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information systems research*, *20*(1), 79-98.

Datareportal (2022). *Global social media statistics.* Retrieved from https://datareportal.com/social-media-users

Di Minin, E., Fink, C., Hausmann, A., Kremer, J., & Kulkarni, R. (2021). How to address data privacy concerns when using social media data in conservation science. *Conservation Biology*, *35*(2), 437-446.

Forbes (2022). *The Top Security Threats of 2022.* Retrieved from https://www.forbes.com/sites/splunk/2022/03/01/the-top-security-threats-of-2022/?sh=4315d2a12e5d

Fox, A. K., & Royne, M. B. (2018). private information in a social world: assessing consumers' fear and understanding of social media privacy. *Journal of Marketing Theory and Practice*, *26*(1-2), 72-89.

Hong, W., & Thong, J. Y. (2013). Internet privacy concerns: an integrated conceptualization and four empirical studies. *MIS Quarterly*, *37*(1), 275-298.

Jain, A. K., Sahoo, S. R., & Jyoti, K. (2021). Online social networks security and privacy: Comprehensive review and analysis. *Complex & Intelligent Systems*, *7*(5), 2157-2177. doi:http://dx.doi.org/10.1007/s40747-021-00409-7

Johansen A. (2022). Tips for protecting your social media privacy. *NortonLifeLock*. Retrieved from https://us.norton.com/internetsecurity-privacy-protecting-privacy-social-media.html

Koohang, A., Floyd, K., Yerby, J., Paliszkiewicz, J (2021). Social media privacy concerns, security concerns, trust, and awareness: Empirical validation of an instrument. Issues in Information Systems, 22(2), 133-145. doi:https://doi.org/10.48009/2_iis_2021_136-149

Koohang, A., Paliszkiewicz, J., & Goluchowski, J. (2018). Social media privacy concerns: trusting beliefs and risk beliefs. *Industrial Management & Data Systems*, *118*(6), 1209-1228

Malhotra, N. K., Kim, S.S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research*, *15*(4), 336-355.

Ming, S. S. Y. (2021). Research on Influencing Factors of Information Privacy Concerns of Social Media Users. *Information and Documentation Services*, *42*(3), 94-104.

Norton (n.d.). *11 social media threats and scams to watch out for.* Retrieved from https://uk.norton.com/internetsecurity-online-scams-11-social-media-threats-and-scams-to-watch-out-for.html

Ozdemir, Z. D., Smith, H. J., & Benamati, J. H. (2017). Antecedents and outcomes of information privacy concerns in a peer context: An exploratory study. *European Journal of Information Systems*, *26*(6), 642-660. doi:http://dx.doi.org/10.1057/s41303-017-0056-z

Paramarta, V., Jihad, M., Dharma, A., Hapsari, I. C., Sandhyaduhita, P. I., & Hidayanto, A. N. (2018). Impact of user awareness, trust, and privacy concerns on sharing personal information on social media: Facebook, Twitter, and Instagram. In *2018 International Conference on Advanced Computer Science and Information Systems (ICACSIS)* (pp. 271-276). IEEE.

Rotter, J. B. & Stein, D. K. (1971). Public attitudes toward the trustworthiness, competence, and altruism of twenty selected occupations. *Journal of Applied Social Psychology, 1*(4), 334-343. available at: https://doi.org/10.1111/j.1559-1816.1971.tb00371.x

Rousseau, D. M., Sitkin, S. B., Burt, R. S., & Camerer, C. (1998). Not so different after all: A cross discipline view of trust. *Academy of Management Review, 23,* 393–404.

Shaw, R. S., Chen, C. C., Harris, A. L., & Huang, H. J. (2009). The impact of information richness on information security awareness training effectiveness. *Computers & Education, 52*(1), 92-100.

Smith, H. J., Dinev, T. & Xu, H. (2011). Information privacy research: an interdisciplinary review. *MIS Quarterly, 35*(4), 980-1016.

Stevens, J. P. (2012). Applied multivariate statistics for the social sciences. Routledge.

Stone, E. F., Gueutal, H. G., Gardner, D. G., & McClure, S. (1983). A field experiment comparing information-privacy values, beliefs, and attitudes across several types of organizations. *Journal of Applied Psychology, 68*(3), 459–468. https://doi.org/10.1037/0021-9010.68.3.459

Wang, L., Sun, Z., Dai, X., Zhang, Y., & Hai-hua Hu. (2019). Retaining users after privacy invasions: The roles of institutional privacy assurances and threat-coping appraisal in mitigating privacy concerns. *Information Technology & People, 32*(6), 1679-1703. doi:http://dx.doi.org/10.1108/ITP-01-2018-0020

Wilson, M., & Hash, J. (2003). Building an information technology security awareness and training program. *NIST Special Publication, 800*(50), 1-39.

Yerby, J., Koohang, A., & Paliszkiewicz, J. (2019). Social media privacy concerns and risk beliefs. *Online Journal of Applied Knowledge Management*, 7(1), 1-13.

Young, A. L., & Quan-Haase, A. (2013). Privacy Protection Strategies on Facebook. *Information, Communication & Society, 16*(4), 479–500. doi:10.1080/1369118x.2013.7777

Zhou, T. (2020). The effect of information privacy concern on users' social shopping intention. *Online Information Review, 44*(5), 1119-1133. doi:http://dx.doi.org/10.1108/OIR-09-2019-0298