ISBN 978-623-99026-6-7

Users' Behavior of Identity Protection and Online Data Security Management

Noah Anburaj Balraj[1,*] & Stanislav Kirilov[2]
[1,2]Asia-Pacific International University
[*]Coresponding author: noah@apiu.edu

Abstract

The objective of this study was to understand the user's IT knowledge to account and data management practices related to personal, social, and business. Internet is global and the vulnerability is global too. The Internet has become part of the people who are engaged with it. The purpose of the study was to learn the level of users' IT knowledge through the account, identity protection, and online data management practices to understand the relationship and design the needed programs to enhance their knowledge for better protection. With the increase in users of mobile phones, laptops, desktops emerge issues and development measures. The identified gap was between the users' IT knowledge and their practices on account and data management. This gap was identified to help design programs to help the users to develop strategies through various alternatives to prevent identity and data theft. The population of data was collected in AIU for strengthening in protecting identity theft and data theft of our faculty members, staff members, students, and other stakeholders. Two samples Chi-Square was used for the analysis of data for the rejection or acceptance of null or alternate hypotheses based on critical value using Microsoft excel. The analysis was individually done for all the 27 factors considered in this research. Results show eight factors had a significant relationship, and 19 factors do not significantly relate between users' IT knowledge and data management and practices. A follow-up study will be conducted on the sub-ordinate level of users' behavior and practice of identity theft and data protection.

Keywords: User experience, identity protection, online data management and practices

INTRODUCTION

Data identity theft is largely a universal issue that is surfacing to consumers' notice. According to a study in the U.S., seven percent of the users were victims of one or more occasions of identity theft in 2014 (Harrell, 2014). This fact is just the identified one, but usually, the facts are well concealed from the users. If we know the unknown, the percentage of identity theft might rise exponentially. I don't think only some are victimized. The service providers have all the data in their storage devices (JRE Clips, 2019). Human behavior is concocted with good and evil. There is a tendency to retain both good and evil behavior for an advantage to accomplish a goal. The display of right ethics shown by service providers makes users believe that the security of identity and data are secured. But on the other hand, the underplayed or unspoken reality to use user identity and data for their business proposition wears down the user trust in the service providers. Aired issues on identity theft and data theft are often reported and interrogated by developed countries.

Mostly, these issues were informed to the rest of the world by the U.S. Traditional crime is now on an e-platform with more informed data on identity and social media platforms (Irshad & Soomro, 2018). As convenience is brought to the use of products and services, consumers show favorable buying behavior. The same convenience of these online platforms gives increasing leverage for criminals to steal users' identities for their business and earnings. Criminals on the new platforms. People are tempted to do wrong. Some yield, and others overcome. As generations come and go, so do criminals. But the crimes appear in the new formats of greater impact related to the online system's outcome.

Mobile and computer users' data spreads far and wide based on their usage of search online. Users' internet activity is automatically stored in the internet-connected databases (***The Growing Concern of Data Theft - Official Site-Flip EBook Pages 1 - 11| AnyFlip | AnyFlip***, n.d.). This might result in severe security problems affecting the tech world. As issues get solved, new issues arise with increased diversity and intensities. Due to less infrastructure, centralized cloud storage share and using data provided minimum security support (Kavitha & Lalitha, n.d.). Social media soon became a tool for data identity theft involving personal data for various threats, abuses, and self-exposure, making it a lot easier to steal data (Vella, 2020). Users are in the queue waiting for their turn in losing the data and identity of the criminals. (Vella, 2020). User data are increasingly vulnerable and exposed to attackers on a daily basis (Venkatesh et al., 2021).

Objective of the Study

To understand users' IT knowledge in data management practices related to personal, social, and business accounts.

Purpose of the Study

The purpose of the study was to learn the level of users' IT knowledge through the account and data management practices to understand the relationship and design needed for formulating a program to enhance users' knowledge of data and identity theft protection management. This study was done at Asia-Pacific International University, Thailand.

Problem Statement

The world has gone into using different platforms for communication and data storage. The behavior of data-stealing, selling, and misusing is on the rise in proportionate to the growth of the IT sector. With the increase in users of mobile phones, laptops, desktops emerge issues and development measures. The identified gap was between the users' IT knowledge and their practices on account and data management. To design enriching programs for the users to learn to develop strategies through various alternatives to prevent identity and data theft. User behavior depends on the IT knowledge procured and used in daily life. Most users don't even know how their stored and daily conversational data is being spied on and stolen (JRE Clips, 2019) (WWLTV, 2019). The professionalism of companies like Facebook and Instagram is honest with the consumers in areas related to consumers' needs/wants. It arose inquisitiveness to advance in research on data and identity theft and devise measures to prevent them.

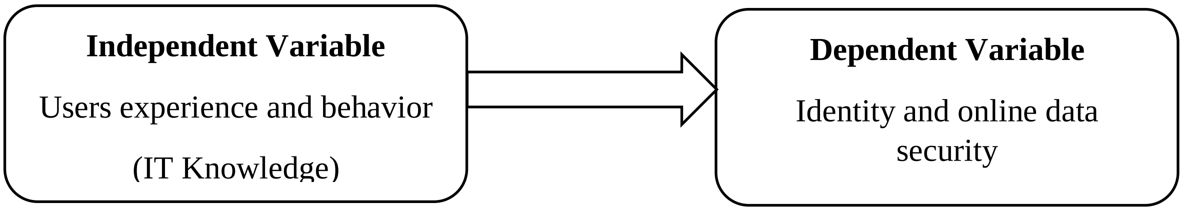
LITERATURE REVIEW

Today’s products are like mobile phones, laptops, desktops, which are all connected to the internet and are vulnerable to others' views. A user of these products does not control the product completely. Users might own them, but the control is subject to the service providers, data and identity thieves, government, and internet service providers. The users may not know the different layers of threats hidden behind the devices or the whole system involved. It is a mystery to many users. An IT professional might have learned the technical know-how but may not be in the motive of the major players involved in doing this IT business. Knowledge of IT products and services is essential for decision making in the purchase, consumption of the applications, and retention of identity and data security, knowledge matters (Park & Moon, 2003). The level of user dependence on cloud storage for eliminating identity and data theft is also dependent on the security technology (Decoy or any other) effective functionality (Kavitha & Lalitha, n.d.). Internet knowledge helps users to opt for the use of the right applications and restrictions of availability online for vulnerability (Wei & Zhang, 2008).

Securing sustainability depends on the users’ knowledge growth (Song, 2002). Innovation and disruptive based growths of IT business relating to other businesses require constant learning of the changing technological world. On the brighter side, the user’s right IT cognitive ability, and on the dark side, predatory behaviors estimate the user’s risk of identity and data theft (Cremer et al., 2016). A study on relationship quality toward internet service providers reveals female users’ trust commitment to loyalty was stronger than male users, while trust in loyalty was stronger for males (Cowley & Mitchell, 2003). Human creation of a genuine environment of trust by the internet service providers will result in increased service users. Data integrity attackers are intelligent on system functionality attacking the cyber networks (Sridhar & Manimaran, 2010). As analysts, we tend to cross-think the growth of the technological world in internet security is a major contribution of cyber attackers and violators. The dark side is brighter in its version to outrun the brighter side. Both these sides have a common goal of earning through technology. The brighter side differs only by being a legalized criminal than their counterparts. Consumer behavior change brought by the digital age makes them digitized and loads tasks such as data generation and management in favor of service providers for their prosperity (Saura et al., 2020).

Conceptual Framework

The developed conceptual framework is simple to the objective of this study. The purpose of this framework is to understand the influence and relationship between user behaviors’ IT knowledge and their account and data management practices.


Independent Variable
Users experience and behavior
(IT Knowledge)
Dependent Variable
Identity and online data security

The hypothesis of the Study

The hypothesis of the study was to demonstrate the existing influence and relationship between user behaviors' IT knowledge and identity and data management practices.

H0: User behavior's IT knowledge is not related to identity and data management practices.
H1: User behavior's IT knowledge is significantly related to identity and data management practices.

Twenty-seven factors were considered in measuring personal, social, business accounts. These factors are shown in Tables 1, 2, 3, and in Table 4, the summary of the three accounts for its level of significance.

Research Methods

This research was intended to measure the relationship between user experiences and behavior towards Identity protection and online data security. The population of this research considered the members of AIU—faculty members, staff members, students, and other stakeholders. The sample includes at least a minimum of 500. The research instrument, a questionnaire of categorical data of yes/no, was used for data collection. The questionnaire was designed to accommodate 27 different factors needed for estimating the user account and data management practices. The questionnaire includes user management and practices of identity and data protection management. Two samples Chi-Square was used for the analysis of data for the rejection or acceptance of null or alternate hypotheses using Microsoft excel. The data were analyzed individually for all 27 factors considered in this research. The hypothesis was tested for its relationship between users' IT knowledge and data management practices in reference to the following considerations: significance level of 0.05, degree of freedom, critical value, p-value, and Chi-Square value.

RESULTS AND DISCUSSIONS

Table 1: Personal data on user experience and behavior on identity and data protection response in percent

No	Factors	Favored %	Not favored %
1	Workshop	61.2	38.8
2	self-learning	70.2	29.8
3	Min. knowledge	47.0	53.0
4	Right personal data for opening accounts	68.3	31.7
5	Sign with Google	69.3	30.7
6	Use Diff. PW	63.2	36.8
7	SSO	52.7	47.3
8	Fingerprint or Facial Recognition	56.4	43.6
9	Pin code	48.0	52.0
10	OTP Authentication	67.2	32.8

11	Online file storage	75.5	24.5
12	Store offline	71.1	28.9
13	One place storage	69.8	30.2
14	Lost data once hardware issues	40.9	59.1
15	Lost data - virus/hacker	26.7	73.3
16	Experience taught me data protection	66.5	33.5
17	Always-on consumer	65.3	34.7
18	Bus App installed	51.3	48.7
19	Off guard during pandemic	45.8	54.2
20	Trust ISS	34.2	65.8
21	Have antivirus - computer	67.2	32.8
22	Antivirus - mobile	39.8	60.2
23	Given PW to imposter	27.0	73.0
24	Suspect OSP	60.9	39.1
25	I do not give real ID for accounts	39.9	60.1
26	Privacy needed	92.2	7.8
27	Personal Id is not for IT companies	84.0	16.0

Table 1 shows the user's behaviors of identity protection and data security related to personal accounts. There are 27 factors considered in this research. The respondents' responses are either favor or did not favor the behavioral aspect.

Table 2: Social account data on user experience and behavior on identity and data protection response in percent

No	Factors	Favored %	Not Favored %
1	Workshop	59.1	40.9
2	self-learning	66.9	33.1
3	Min. knowledge	47.2	52.8
4	Right personal data for opening accounts	58.8	41.2
5	Sign with Google	74.0	26.0
6	Use Diff. PW	65.8	34.2
7	SSO	50.6	49.4
8	Fingerprint or Facial Recognition	47.1	52.9
9	Pin code	41.4	58.6
10	OTP Authentication	66.5	33.5
11	Online file storage	68.8	31.2
12	Store offline	61.8	38.2

13	One place storage	58.4	41.6
14	Lost data once hardware issues	35.3	64.7
15	Lost data - virus/hacker	21.3	78.7
16	Experience taught me data protection	65.3	34.7
17	Always-on consumer	65.7	34.3
18	Bus App installed	46.5	53.5
19	Off guard during pandemic	43.8	56.3
20	Trust ISS	32.0	68.0
21	Have antivirus - computer	62.4	37.6
22	Antivirus - mobile	41.4	58.6
23	Given PW to imposter	30.6	69.4
24	Suspect OSP	66.5	33.5
25	I do not give real ID for accounts	46.4	53.6
26	Privacy needed	91.3	8.7
27	Personal Id is not for IT companies	82.1	17.9

Table 2 shows the user's behaviors of identity protection and data security related to social accounts. There are 27 factors considered in this research. The respondents' responses are either favor or did not favor the behavioral aspect.

Table 3: Business account data on user experience and behavior on identity and data protection response in percent

No	Factors	Favored %	Not Favored %
1	Workshop	50.3	49.7
2	self-learning	51.8	48.2
3	Min. knowledge	49.1	50.9
4	Right personal data for opening accounts	57.1	42.9
5	Sign with Google	51.6	48.4
6	Use Diff. PW	65.6	34.4
7	SSO	44.9	55.1
8	Fingerprint or Facial Recognition	35.7	64.3
9	Pin code	38.4	61.6
10	OTP Authentication	60.1	39.9
11	Online file storage	67.3	32.7
12	Store offline	64.1	35.9
13	One place storage	58.1	41.9
14	Lost data once hardware issues	25.5	74.5
15	Lost data - virus/hacker	12.2	87.8
16	Experience taught me data protection	62.3	37.7
17	Always-on consumer	52.2	47.8

18	Bus App installed	54.1	45.9
19	Off guard during pandemic	40.8	59.2
20	Trust ISS	31.0	69.0
21	Have antivirus - computer	62.6	37.4
22	Antivirus - mobile	38.2	61.8
23	Given PW to imposter	19.7	80.3
24	Suspect OSP	54.2	45.8
25	I do not give real ID for accounts	36.4	63.6
26	Privacy needed	87.4	12.6
27	Personal Id is not for IT companies	75.6	24.4

Table 3 shows the user's behaviors of identity protection and data security related to business accounts. There are 27 factors considered in this research. The respondents' responses are either favor or did not favor the behavioral aspect.

Table 4: Critical value and p-value for rejection or acceptance of null or alternate hypothesis

No	**Factors**	**Significance**	**Degree of Freedom**	**Critical Value**	**P-value**	**Chi-Square**	**Null Hypothesis Accepted/ Rejected**
1	Workshop	0.05	2	5.99	0.0932	4.72	**Accepted**
2	self-learning	0.05	2	5.99	0.0007	14.28	Rejected
3	Min. knowledge	0.05	2	5.99	0.9143	0.18	**Accepted**
4	Right personal data for opening accounts	0.05	2	5.99	0.054675	6.06	Rejected
5	Sign with Google	0.05	2	5.99	0.000030	20.49	Rejected
6	Use Diff. PW	0.05	2	5.99	0.838625	0.35	**Accepted**
7	SSO	0.05	2	5.99	0.324826	2.27	**Accepted**
8	Fingerprint or Facial Recognition for login	0.05	2	5.99	0.000479	17.70	Rejected
9	Pin code	0.05	2	5.99	0.157758	3.71	**Accepted**
10	OTP Authentication	0.05	2	5.99	0.329753	2.16	**Accepted**
11	Online file storage	0.05	2	5.99	0.179516	3.59	**Accepted**
12	Store offline	0.05	2	5.99	0.139948	4.07	**Accepted**
13	One place storage	0.05	2	5.99	0.027809	7.54	Rejected

14	Lost data once hardware issues	0.05	2	5.99	0.010088	10.04	Rejected
15	Lost data - virus/hacker	0.05	2	5.99	0.003311	14.35	Rejected
16	Experience taught me data protection	0.05	2	5.99	0.71176	0.67	**Accepted**
17	Always-on consumer	0.05	2	5.99	0.015923	8.09	Rejected
18	Bus App installed	0.05	2	5.99	0.390363	1.89	**Accepted**
19	Off guard during pandemic	0.05	2	5.99	0.637655	0.91	**Accepted**
20	Trust ISS	0.05	2	5.99	0.805644	0.43	**Accepted**
21	Have antivirus - computer	0.05	2	5.99	0.547416	1.23	**Accepted**
22	Antivirus - mobile	0.05	2	5.99	0.837129	0.36	**Accepted**
23	Given PW to imposter	0.05	2	5.99	0.073408	5.74	**Accepted**
24	Suspect OSP	0.05	2	5.99	0.080149	5.10	**Accepted**
25	I do not give real ID for accounts	0.05	2	5.99	0.177708	3.46	**Accepted**
26	Privacy needed	0.05	2	5.99	0.284052	2.29	**Accepted**
27	Personal Id is not for IT companies	0.05	2	5.99	0.116431	4.04	**Accepted**

Table 4 shows the result of all 27 factors considered in the data analysis. The reason for individually analyzing the factors was to specifically identify each factor of their relationship or no relationship between user behavior and IT knowledge on their different accounts management and practices executed for identity protection and data security. Compared test statistics and critical values for all 27 factors administered. The critical value = 5.99, and the $\chi 2$ value range is from 0.18 to 20.49.

Factors like self-learning (14.28), opening accounts with correct personal data (6.06), signing with Google (20.49), use of a pin or facial recognition for login additional to PW (17.70), one place storage (7.54), lost data at least once because of hardware malfunction (10.04), lost data at least once because of virus/hackers (14.35), and always on consumers (8.09), for these factors, the Chi-Square $\chi 2$ value is above the critical value of 5.99; therefore, the null hypothesis was rejected, and alternate hypothesis was accepted-- H1: User behavior's IT knowledge is significantly related with account and data management practices.

Factors like a workshop (4.72), minimum knowledge (0.18), using different passwords (0.35), single sign-on (2.27), pin code used for login (3.71), OTP authentication (2.16), online file storage

(3.59), store offline (4.07), the experience taught me data protection (0.67), a business app installed (1.89) off guard during pandemic (0.91), trust ISS (0.43), have antivirus in computer (1.23), antivirus in mobile (0.36), given PW to imposter at least once (5.74), suspicion of OSP is shown (5.10), I do not give real ID for accounts (2.29), and I don't like to give personal Id to IT companies (4.04), all these factors Chi-Square $\chi 2$ value is below the critical value of 5.99. Therefore, the null hypothesis was accepted—H_0: User behavior's IT knowledge is not related to account and data management practices.

Implication

The managerial implications of this research emphasize its factors for its significance related to identity and data management practices. The results address the need level for training and development of users for better security. The respondents' behaviors accounted for designing training/orientation programs. Training programs should be designed and customized according to the level of IT knowledge exhibited in the results. A note of caution on the respondents' actual vs. future need reality.

CONCLUSION

Users' IT knowledge certainly influences data management and practices. There would be no significant data management and practices without the IT knowledge of the users. Significant influence of users' knowledge helps users to be smart in data management and practices. The increased development of the IT industry in almost all walks of human living greatly demands the increase of the user's IT knowledge on a continuous basis. Data management and practices should be designed rather than letting users flow along with the current. There is a number of reasons for identity protection and data security, namely, the internet is global, internet users are varied like imposters/hackers, online service providers, marketers looking for consumer behaviors data on product/service purchase and consumption, IT companies, governments, and artificial intelligence developers. Thus, an individual's identity protection and data security practices are vulnerable to exploitation.

Recommendation

1. To recommend AIU for implementing an awareness training program
2. To create enthusiasm and interest in users to take responsibility to protect their identity and data.
3. Design orientation program for users of mobile and PCs enhancing their data management practices.
4. To recommend AIU to take measures for privacy, identity, and data security.

REFERENCE

Cowley, E., & Mitchell, A. A. (2003). The Moderating Effect of Product Knowledge on the Learning and Organization of Product Information. *Journal of Consumer Research*, *30*(3), 443–454. https://doi.org/10.1086/378620

Harrell, E. (2014). *Victims of Identity Theft, 2014*. 26.

Irshad, S., & Soomro, T. R. (2018). *Identity Theft and Social Media*. 14.

JRE Clips. (2019, October 23). *Edward Snowden: How Your Cell Phone Spies on You*. https://www.youtube.com/watch?v=VFns39RXPrU

Kavitha, O., & Lalitha, D. B. (n.d.). *Data theft protection in cloud storage using Decoy technology*. *0886*, 7.

Park, C.-W., & Moon, B.-J. (2003). The relationship between product involvement and product knowledge: Moderating roles of product type and product knowledge type. *Psychology & Marketing*, *20*(11), 977–997. https://doi.org/10.1002/mar.10105

Saura, J. R., Reyes-Menendez, A., Matos, N. de, Correia, M. B., & Palos-Sanchez, P. (2020). Consumer Behavior in the Digital Age. *Journal of Spatial and Organizational Dynamics*, *8*(3), 190–196.

Song, S. (2002). An Internet Knowledge Sharing System. *Journal of Computer Information Systems*, *42*(3), 25–30. https://doi.org/10.1080/08874417.2002.11647499

Sridhar, S., & Manimaran, G. (2010). Data integrity attacks and their impacts on SCADA control system. *IEEE PES General Meeting*, 1–6. https://doi.org/10.1109/PES.2010.5590115

The Growing Concern of Data Theft - Official Site-Flip eBook Pages 1 - 11| AnyFlip | AnyFlip. (n.d.). Retrieved October 21, 2021, from http://anyflip.com/igbl/dgic/basic

Vella, E. (2020). (2020). *Is data theft from social media a preparatory act for other crimes? : the Maltese experience*. https://www.um.edu.mt/library/oar/handle/123456789/77352

Venkatesh, S. V., Prasannakumaran, D., Bosco, J. J., Kumaar, R. P., & Vijayaraghavan, V. (2021). A Non-intrusive Machine Learning Solution for Malware Detection and Data Theft Classification in Smartphones. In M. Paszynski, D. Kranzlmüller, V. V. Krzhizhanovskaya, J. J. Dongarra, & P. M. A. Sloot (Eds.), *Computational Science – ICCS 2021* (pp. 200–213). Springer International Publishing. https://doi.org/10.1007/978-3-030-77967-2_17

Wei, L., & Zhang, M. (2008). The Impact of Internet Knowledge on College Students' Intention to Continue to Use the Internet. *Information Research: An International Electronic Journal*, *13*(3). https://eric.ed.gov/?id=EJ837270

WWLTV. (2019, November 1). *Is my phone listening to me? We tested it, here's what happened*. https://www.youtube.com/watch?v=CVazBWGgg64