Webology (ISSN: 1735-188X)
Volume 19, Number 2, 2022

Responsible Digital Citizenship: A Measurement Of Trust In The World Wide Web

Dave E. Marcial[1] , Jan Cynth Palama[2] , Aurielle Lisa Maypa[3] , Markus A. Launer[4]

[1, 2, 3] Silliman University, Philippines.

[4] Ostfalia University of Applied Sciences, Germany.

ABSTRACT

The Internet is a powerful platform in the workplace. However, when abused, it is a place that destroys everyone. This paper presents how society is practicing netizenship responsibility. Specifically, it measures trust towards the Internet and social media as perceived by the employees. It also describes predictors that affect confidence level on the Internet and social media trust. A total of 5146 were analyzed from 36 countries. An online survey questionnaire was used utilizing the Marcial-Launer Digital Trust in the Workplace Questionnaire. Results show that the overall mean of the agreement level on Internet trust is moderate ($\overline{x}$ = 2.59). It also shows that age, gender, continent, innovation index, income level, social technologic ladder, internet satisfaction, job position, company form, company role, and company size were significant predictors of Internet trust. It is concluded that citizens have reasonable confidence that society is doing responsible citizenship. There is a need to establish an ecosystem that can be digitally trusted.

Keywords: digital trust, Internet trust, responsible use of social media, netizenship

INTRODUCTION

The World Wide Web, web in short, “a set of software services running on the Internet” (Diffen, 2012), provides an array of information retrieval services of the Internet (The Editors of Encyclopaedia Britannica, 2019). It is an invention that connects the world in three ways (Google Arts and Culture, n.d.). First, it allows us to locate vast information on the Internet through a uniform resource locator (URL), the addressing scheme to find a document. Second, it allows computers to connect and search hypermedia documents that feature links to images, sounds, animations, and movies through the hypertext transfer protocol (HTTP). Lastly, it stimulates human-computer interaction through the hypertext markup language (HTML) that arranges pages holding hypertext links. Through browser software, users can “share their work and thoughts through social networking sites, blogs, video sharing, and more" (Google Arts and Culture, n.d.). In short, the World Wide Web changes the way people search and reuse information, interact and communicate, do business (BBC News, 2019).

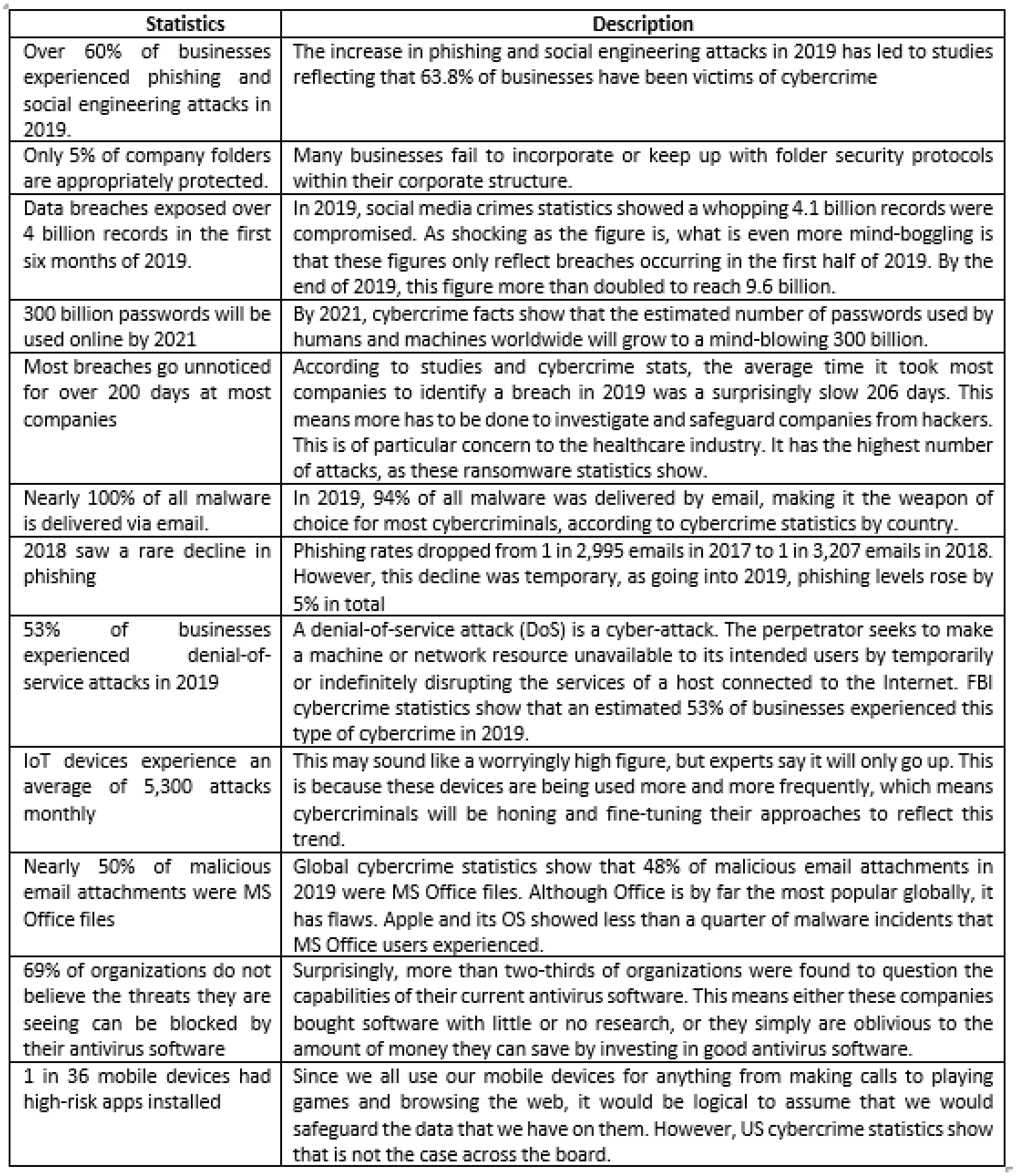
The web is evolving rapidly from Web 1.0 of the 1980s until the present time called Web 4.0 significantly affects every netizen (Solanki & Dongaonkar, 2016) (Choudhury, 2014). Web 4.0 is a product of today's Fourth Industrial Revolution, highlighting the "fusion of technologies that is blurring the lines between the physical, digital, and biological spheres" (Schwab, 2016). These technologies evolve exponentially in velocity, scope, and systems impact that challenge every business, government, and people (Schwab, 2016).

However, statistics show that people continue to question its trust on the web. It is a place for cybercrimes and data breaches. Among these worrying statistics, as summarized in (Lazic, 2021), are shown in table 1.

These statistics will lead every netizen to question, how safe are we on the world wide web? How secure are our data and information in the workplace? What are the practices of businesses, our government, and very netizen regarding the world wide web? Are our companies, government, and fellow citizens performing responsible digital citizenship? Moreover, above all, are we trusting our company, government, and fellow compatriots in terms of their Internet usage and practices?

"Digital citizenship is the ability to safely and responsibly access digital technologies, as well as being an active and respectful member of society, both online and offline" (FutureLearn, 2021). To foster digital citizenship, safe and responsible use of the Internet and social media, everyone should practice (APEID-ICT in Education, UNESCO Asia-Pacific Regional Bureau of Education, 2015). Digital citizens must responsibly "engage in a wide range of activity from creating, consuming, sharing, playing and socializing, to investigating, communicating, learning and working" (Richardson & Milovidov, 2019). The International Society for Technology in Education describes digital citizens as follows: a) use technology to make the community better, b) engaged online with respect regardless of beliefs, c) utilize technology to be heard by the government and demonstrate public policy d) validates and verify online sources of information (International Society for Technology in Education (ISTE), n.d.).

Table 1. Cybercrime Statistics (Lazic, 2021)



Statistics	Description
Over 60% of businesses experienced phishing and social engineering attacks in 2019.	The increase in phishing and social engineering attacks in 2019 has led to studies reflecting that 63.8% of businesses have been victims of cybercrime
Only 5% of company folders are appropriately protected.	Many businesses fail to incorporate or keep up with folder security protocols within their corporate structure.
Data breaches exposed over 4 billion records in the first six months of 2019.	In 2019, social media crimes statistics showed a whopping 4.1 billion records were compromised. As shocking as the figure is, what is even more mind-boggling is that these figures only reflect breaches occurring in the first half of 2019. By the end of 2019, this figure more than doubled to reach 9.6 billion.
300 billion passwords will be used online by 2021	By 2021, cybercrime facts show that the estimated number of passwords used by humans and machines worldwide will grow to a mind-blowing 300 billion.
Most breaches go unnoticed for over 200 days at most companies	According to studies and cybercrime stats, the average time it took most companies to identify a breach in 2019 was a surprisingly slow 206 days. This means more has to be done to investigate and safeguard companies from hackers. This is of particular concern to the healthcare industry. It has the highest number of attacks, as these ransomware statistics show.
Nearly 100% of all malware is delivered via email.	In 2019, 94% of all malware was delivered by email, making it the weapon of choice for most cybercriminals, according to cybercrime statistics by country.
2018 saw a rare decline in phishing	Phishing rates dropped from 1 in 2,995 emails in 2017 to 1 in 3,207 emails in 2018. However, this decline was temporary, as going into 2019, phishing levels rose by 5% in total
53% of businesses experienced denial-of-service attacks in 2019	A denial-of-service attack (DoS) is a cyber-attack. The perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting the services of a host connected to the Internet. FBI cybercrime statistics show that an estimated 53% of businesses experienced this type of cybercrime in 2019.
IoT devices experience an average of 5,300 attacks monthly	This may sound like a worryingly high figure, but experts say it will only go up. This is because these devices are being used more and more frequently, which means cybercriminals will be honing and fine-tuning their approaches to reflect this trend.
Nearly 50% of malicious email attachments were MS Office files	Global cybercrime statistics show that 48% of malicious email attachments in 2019 were MS Office files. Although Office is by far the most popular globally, it has flaws. Apple and its OS showed less than a quarter of malware incidents that MS Office users experienced.
69% of organizations do not believe the threats they are seeing can be blocked by their antivirus software	Surprisingly, more than two-thirds of organizations were found to question the capabilities of their current antivirus software. This means either these companies bought software with little or no research, or they simply are oblivious to the amount of money they can save by investing in good antivirus software.
1 in 36 mobile devices had high-risk apps installed	Since we all use our mobile devices for anything from making calls to playing games and browsing the web, it would be logical to assume that we would safeguard the data that we have on them. However, US cybercrime statistics show that is not the case across the board.

However, achieving digital citizenship challenges everyone. Digital citizenship is not just about personal responsibility. It involves nine elements. These are digital access, etiquette, law, communication, digital literacy, digital commerce, digital rights and responsibilities, digital safety and security, and digital health and wellness (Ribble, 2021). “Competent digital citizens are able to respond to new and everyday challenges related to learning, work, employability, leisure, inclusion and participation in society, respecting human rights and intercultural differences” (Richardson & Milovidov, 2019). It needs a certain level of trust to foster digital citizenship. Trust is considered as of the significant factors in developing a healthy digital culture in society (Marcinek, 2014). “It is a foundation of serving citizens in a digital world” (Conrad & Combs, 2017). The United Nations Conference on Trade and Development explained that “more trust in the internet is needed if the digital economy is to become a viable development tool for developing nations” (UNCTAD, 2019). Among the many strategies to build Internet trust among citizens include: a) technology baselining, b) digital empowerment, c) communicating benefits, d) transparency, and e) privacy and security assurance (Conrad & Combs, 2017). Digital citizenship, specifically responsible use of the Internet and social media, was proposed as one of the critical elements in building digital trust in IT processes (Marcial & Launer, Towards the Measure of Digital Trust in the Workplace: A Proposed Framework, 2019).

This article describes responsible digital citizenship in the workplace. Specifically, this article measures the confidence level towards using the Internet and social media in society as perceived by the employees. It also presents the relationships and differences between Internet trust and the respondents’ socio-demographics, employment, and technological profile. This paper is part of the global study on the “Measurement of Digital Trust in the Workplace” (Marcial & Launer, Towards the Measure of Digital Trust in the Workplace: A Proposed Framework, 2019).

METHODS

Datasets were extracted from Marcial and Launer’s Survey 2020 data on Digital Trust in the Workplace. An online survey was conducted in different sectors from 36 countries in Europe, the USA, Latin America, Africa, and Asia. A total of 5146 responses were included in the analysis (Marcial & Launer, Test-retest Reliability and Internal Consistency of the Survey Questionnaire on Digital Trust in the Workplace, 2021).

One of the sections of the survey questionnaire is digital citizenship. It has ten statements about the responsible use of the Internet and social media. Respondents were asked their level of agreement with the statements. A 4-point Likert scale is used: 1=strongly disagree, 2=disagree, 3 = agree, and 4=strongly agree. Similarly, the survey questionnaire collected socio-demographic, employment, and technological profiles.

The demographic profiles include the respondent’s age range, gender, civil status, and highest educational attainment. Likewise, it also includes the continent where the respondent is working, the respondents’ country’s innovation index, the respondents’ country, and the income level of the respondents’ country. Age ranges 18 or younger (1), 19 – 28 (2), 29 – 38 (3), 39 – 48 (4), 49 – 58 (5), and 59 and older (6). Gender is categorized into 3: 1 (female), 2 (LGBT-Q), and 3 (male). Status is categorized into a single (1), married (2), separated or divorced (3), widowed 4). The education is coded into 1 = post-doctoral, 2 = post-graduate, 3 = graduate, 4 = bachelor’s degree, 5 = technical, vocational, or skill diploma, 6 = middle/senior high school diploma, 7 = junior high school diploma, 8 = elementary diploma, and 9 = primary diploma. The continent was coded based on WorldAtlas [1]. As published, “only countries recognized by the United Nations are listed, not dependencies and/or territories.” Income level was coded based on the World Bank [2]. The innovation index was assigned based on the Global Innovation Index [3].

Employment profile includes respondent’s years of working experience, employment status, job position, company type, company form, company role, and size of the company. Employment status was coded as 1 = regular or permanent and 2 as probationary or temporary. The job position is 1 for Top Management like CEO, President, Board Members, Vice Presidents, 2 for Middle Management like Department Heads, Branch Managers, 3 for First Level Management like Supervisors, Foreman, Office Managers, 4 for Contributors like Salesmen, Clerical, Secretarial, Technical Employees, and 5 for self-employed. Company type is coded as 1 for Private, 2 for government, 3 for Non-government, 4 for Semi-private and semi-government, and 5 for business with one person. Company form is 1 for virtual like digital organization, network organization or modular organization, and 2 for non-virtual like the classic onsite company. Company size is coded as 1 for small enterprises with 1 to 10 employees, medium-sized with 1 to 500 employees, 3 for large enterprises with 501 to 200 employees, 4 for small groups with more than 2000 employees but less than 10000, and 5 for large groups with over 10000 employees.

Social technologic profiles and internet satisfaction comprises the technological profile of the respondents. The social technologic ladder was coded based on the 2007 Forster Social Technologic Profile as follows 1 = CREATORS (monthly, publishes blogs and websites, uploads videos you created, uploads audio/music you created, writes articles or stories and posts them online, 2 = CONVERSATIONALISTS (weekly, updates the status on a social networking site, posts updates on Twitter), 3 = CRITICS (monthly, posts ratings/reviews of products or services, comments on someone else’s blog, contributes to online forums, and edits articles on a wiki), 4 = COLLECTORS (monthly, uses RSS feeds, vote for websites online, add “tags” to web pages or photos), 5 = JOINERS (monthly, maintains a profile on a social networking site and visits social networking sites, 6 = SPECTATORS (monthly, reads blogs, listens to podcasts, watches a video from other users, reads online forums, consumer ratings/reviews, and tweets), and 7 = INACTIVES (none of the above). On the other hand, satisfaction level in connecting to the Internet is coded as 1 = not satisfied, 2 = slightly satisfied, 3 = moderately satisfied, 4 = extremely satisfied, and 5 = not applicable (I have not availed of these services). Years in the company are assigned with 1 (less than 1 year), 2 (1-3 years), 3 (4-10 years), 4 (11-20 years), 5 (21-30 years), 6 (31 – 40 years), 7 (more than 40 years).

The following statistical tools were utilized in this paper: overall mean to determine the trust level, chi-square, and multiple regression to determine significant relationships, and One-way ANOVA to estimate significant differences. MS Excel, particularly pivot table and data analysis features, were used during the calculations.

RESULTS

Internet Trust Level

Table 2. Internet and Social Media Use

Statements on the Use of Internet and social media		Level of Agreement	
		x̲	Description
a	registering with a Web site (i.e., giving my name, email address, medical registration number, etc.) may enable that site to keep track of what I view or spend online.	3.14	Agree
b	information given to a company website will not be passed on to third parties.	2.47	Disagree
c	my web-browsing habits are not being tracked.	2.40	Disagree
d	that providing personal information in social media is safe.	2.36	Disagree
e	my co-workers do not spread unverified information on social media – especially those that do nothing but provoke fear in the community.	2.73	Agree
f	my co-workers do not post information on social media, which would tend to worsen the situation.	2.76	Agree
g	my countrymen use confidential information when absolutely necessary.	2.55	Agree
h	my countrymen understand their responsibilities, and they are responsible netizens.	2.51	Agree
i	my countrymen understand and comply with the data and privacy law.	2.51	Agree
j	my government protects our personal information.	2.48	Disagree
Overall Mean		**2.59**	Agree

As shown in Table 2, the overall mean of 2.59 on the agreement level to the statements on responsible netizenship in society is described as “agree.” Four statements related to online safety and information sharing are described as “disagree.” Specifically, the statement “information given to a company website will not be passed on to third parties” is rated “disagree” with a mean of 2.47. A mean of 2.40 is rated to the statement “my web-browsing habits are not being tracked,” and it is described as “disagree.” The statement” providing personal information in social media is safe” is also described as “disagree” ($\bar{x}$ = 2.36). Surprisingly, a “disagree” rating was given to the statement “my government protects our personal information” with a mean of 2.48.

Demographic Profiles and Internet Trust

Table 3 shows the analysis to ascertain whether or not a significant relationship exists between the respondent's demographic profile and their level of trust in responsible netizenship. It is worth noting that all variables appeared to be significantly related to trust in responsible netizenship in society.

Table 3. Test of Relationship between Demographic Profiles and Internet Trust

Variables	**x^2 Value**	**p-value**	**df**	**Remarks**
Age	509.747	0	15	significant
Status	57.485	0	9	significant
Gender	127.459	0	6	significant
Continent	318.832	0	15	significant
Education	184.669	0	24	significant
Income Level	247.183	0	12	significant

Further, a multiple regression was calculated to predict the Internet trust level of the respondent's age, status, gender, education, country's innovation index, continent, and income level (see Table 4). A significant regression equation was found (F (8), 5137) = 52.97, p < .00), with an R^2 of 0.08. Age, gender, continent, innovation index, and income level were significant predictors of trust level on netizenship. Data shows that the respondent's ages 49 to 58 have moderate Internet trust levels ($\underline{x}$ = 2.79). The same level of trust is also shown with ages 18 or younger ($\bar{x}$ = 2.67), 39-48 ($\bar{x}$ =2.58), 19-25 ($\bar{x}$ =2.56). It is worth noting that the respondents with age brackets 29-38 and 59 or older disagreed on the statements on responsible use Internet and social media with a $\bar{x}$ =2.50 and $\bar{x}$ = 2.49, respectively. Male respondents have a moderate level of confidence on the Internet with a mean of 2.63, and LGBTQ respondents have a trust level of 2.53.

Table 4. Multiple Regression between Internet Trust and Demographic Profiles

Regression Statistics	
Multiple R	0.28
R Square	0.08
Adjusted R Square	0.07
Standard Error	0.71
Observations	5146

ANOVA

	df	SS	MS	F	Significance F
Regression	8	211.87	26.48	52.97	0.00
Residual	5137	2568.40	0.50		
Total	5145	2780.26			

	Coefficients	Standard Error	t Stat	P-value	Lower 95%	Upper 95%	Lower 95.0%	Upper 95.0%
Intercept	2.74	0.07	41.20	0.00	2.61	2.87	2.61	2.87
Age	0.04	0.01	3.71	0.00	0.02	0.06	0.02	0.06
Gender	0.02	0.01	2.11	0.03	0.00	0.04	0.00	0.04
Status	0.00	0.02	-0.21	0.84	-0.04	0.03	-0.04	0.03
Education	0.01	0.01	1.24	0.22	-0.01	0.03	-0.01	0.03
Country	0.00	0.00	0.64	0.52	0.00	0.00	0.00	0.00
Continent	0.03	0.01	3.10	0.00	0.01	0.05	0.01	0.05
Innovation Index	-0.01	0.00	-14.38	0.00	-0.01	0.00	-0.01	0.00
Income Level	-0.14	0.02	-8.12	0.00	-0.17	-0.10	-0.17	-0.10

The result shows that the respondents from low-income countries (x̅ = 2.78), lower middle (x̅ = 2.56), high income (x̅ =2.56) have moderate Internet trust. Respondents from upper-middle-income countries disagree with the statements on the responsible use of the Internet and social media with a mean of 2.36. In terms of continent, the result shows that Asian respondents have the highest mean of Internet trust (x̅ = 2.69), described as moderate. Continents that have a moderate level of Internet trust are Europe (x̅ = 2.67), North America (x̅ = 2.56), South America (x̅ = 2.38), and Oceania (x̅ = 2.34). African respondents disagreed with the statements related to responsible netizenship (x̅ = 2.21).

A one-way ANOVA was conducted to compare the differences of trust level on data protection and privacy on the different demographic profiles (Table 5). An analysis of variance shows that the trust level among the groups of respondents in terms of continent and income level significantly differ. These results are manifested in the p-values, higher than the margin of error at 0.05. This shows that their differences in trust level have reached the significance level. Hence, the employee respondents from the different income level with F (4, 45) = 2.65, p = 0.046, and continent with F (5, 54) = 4.13, p = 0.00 differ.

Table 5. Test of Difference of trust level among the groups of respondents according to their demographics

Socio-demographics	F	p-value	Remarks
by age range	2.26	0.06	not significant
by gender	0.55	0.58	not significant
by status	1.40	0.26	not significant
by educational attainment	1.00	0.45	not significant
by continent	4.13	0.00	significant
by income level	2.65	0.05	significant

Technologic Profile and Internet Trust

Table 6 shows the results of the analysis made to ascertain whether or not a significant relationship exists between the respondent's demographic profile and their level of trust in responsible netizenship. Results show that the social technologic ladder and internet satisfaction are significantly related to trust in responsible netizenship in society. Similarly, the multiple regression resulted in the social technologic ladder and level of internet satisfaction being significant predictors of trust level on responsible netizenship, shown in Table 7. A significant regression equation was found (F (2), 5143) = 612.50, $p < .00$), with an R^2 of 0.19.

Table 6. Test of Relationship between Demographic Profiles and Internet Trust

Variables	x2 Value	P-Value	df	Remarks
Ladder	617.536	0	18	Significant
Internet Satisfaction	1319.396	0	12	Significant

It denotes that these technological profiles affect the trust level of the employees towards their perception of how the society is implementing responsible netizenship. Notably, employees who are social media creators have the highest mean ($\bar{x}$ = 2.87), interpreted as moderate level. Likewise, the social media critics ($\bar{x}$ =2.67), conversationalists ($\bar{x}$ =2.56), and collectors ($\bar{x}$ = 2.52) have a moderate extent of IT trust. However, employees who described their selves as spectators ($\bar{x}$ =2.41) and inactive ($\bar{x}$ =2.47) disagreed on the responsible use of the Internet and social media statements. Expectedly, those extremely satisfied with their internet connectivity have a better trust level with a mean of 2.80.

Table 7. Multiple Regression between Internet Trust and Technologic Profiles

Regression Statistics	
Multiple R	0.44
R Square	0.19
Adjusted R Square	0.19
Standard Error	0.66

Observations	5146

ANOVA

	df	SS	MS	F	Significance F
Regression	2	534.83	267.42	612.50	0.00
Residual	5143	2245.43	0.44		
Total	5145	2780.26			

	Coefficients	Standard Error	t Stat	P-value	Lower 95%	Upper 95%	Lower 95.0%	Upper 95.0%
Intercept	1.90	0.04	50.44	0.00	1.83	1.97	1.83	1.97
Social Technologic Ladder	-0.06	0.00	-13.05	0.00	-0.07	-0.05	-0.07	-0.05
Internet Satisfaction	0.29	0.01	30.14	0.00	0.27	0.31	0.27	0.31

Table 8. Test of Difference of Internet Trust level among the groups of respondents according to their Technologic Profile

Technologic Profile	F	p-value	Remarks
by Social Technologic Ladder	3.71	0.00	significant
by Internet Satisfaction	15.43	0.00	significant

A one-way ANOVA was conducted to compare the differences of trust level on data protection and privacy on the different technologic profiles (Table 8). An analysis of variance shows that the trust level among the groups of respondents in terms of technologic ladder and internet satisfaction significantly differ. These results are manifested in the p-values, which are lower than the error margin at 0.05. This shows that their differences in trust level have reached the significance level. Hence, the employee respondents from the different ladder with F (4, 45) = 3.71, p = 0.00 and internet satisfaction F (4, 45) = 15.43, p = 0.00 differ.

Employment Profile and Internet Trust

Table 9 shows the results of the analysis made to ascertain whether or not a significant relationship exists between the respondent's employment profile and their level of trust in responsible netizenship. Results show that company form, type, size, position, status, and the number of years of working are significantly related to trust in responsible netizenship in society. On the other hand, shown in Table 10, the multiple regression resulted in the respondent's job position, company form, company role, and company size were significant predictors of trust level on responsible netizenship. A significant regression equation was found (F (7), 5146) = 9.27, $p < 0.00$), with an R^2 of 0.01.

Table 9. Test of Relationship between Employment Profiles and Internet Trust

Variables	x2 Value	P-Value	df	Remarks
Organizational Form	29.637	0	3	Significant
Organizational Role/Type	94.256	0	12	Significant
Organizational Size	758.285	0	12	Significant
Company Position	341.212	0	12	Significant
Employment Status	32.623	0	3	Significant
Professional Experience	337.127	0	18	Significant

Table 10. Multiple Regression between Employment Profiles and Internet Trust

Regression Statistics	
Multiple R	0.11
R Square	0.01
Adjusted R Square	0.01
Standard Error	0.73
Observations	5146

ANOVA

	df	SS	MS	F	Significance F
Regression	7	34.67	4.95	9.27	0.00
Residual	5138	2745.59	0.53		
Total	5145	2780.261518			

	Coefficients	Standard Error	t Stat	P-value	Lower 95%	Upper 95%	Lower 95.0%	Upper 95.0%
Intercept	2.58	0.08	32.98	0.00	2.43	2.73	2.43	2.73
Years of Experience	0.01	0.01	0.74	0.46	-0.01	0.03	-0.01	0.03

Employment Status	0.06	0.04	1.81	0.07	-0.01	0.13	-0.01	0.13
Job Position	-0.02	0.01	-2.02	0.04	-0.04	0.00	-0.04	0.00
Company Type	-0.01	0.01	-0.84	0.40	-0.03	0.01	-0.03	0.01
Company Form	-0.12	0.02	-5.05	0.00	-0.17	-0.07	-0.17	-0.07
Company Role	0.04	0.01	5.90	0.00	0.03	0.05	0.03	0.05
Company Size	0.02	0.01	2.38	0.02	0.00	0.04	0.00	0.04

Data shows that the respondents who are in the middle management have the highest mean of Internet trust with a mean of 2.41, who moderately agreed on the statements related to responsible netizenship. The same level of trust goes to first-level managers (x̄ =2.55) and self-employed (x̄ =2.59). However, top managers and contributor employees disagree with the statements on responsible use of the Internet and social media, with a mean of 2.49.

Likewise, the result signifies that company form impacts trust level on data and privacy. It is noted that respondents who work virtually have the highest mean trust (x̄ = 2.65), fall under moderate level. Employees who work onsite also have moderate Internet trust (x̲ = 2.57). Further, the result shows that the number of employees in a workplace affects the trust level on responsible netizenship. Data shows that respondents who work in small group companies have the highest confidence level (x̲ = 2.68) of Internet trust.

A one-way ANOVA was conducted to compare the differences of trust level on data protection and privacy on the different employment profiles (Table 11). An analysis of variance shows that the trust level among the groups of respondents in terms of company type, company size, job position, employment status, and the number of working experiences do not significantly differ. These results are manifested in the p-values, which are lower than the error margin at 0.05. This shows that their differences in trust level have not reached the significance level. Hence, the employee respondents from the different employment profile groups do not differ.

Table 11. Test of Difference of trust level among the groups of respondents according to their Employment Profiles

Employment Profile	F	p-value	Remarks
by Company Type	0.23	0.92	not significant
by Company Size	0.84	0.51	not significant
by Job Position	1.21	0.32	not significant
by Employment Status	0.09	0.76	not significant

by Number of Working Experience	0.60	0.73	not significant

DISCUSSION

The result implies that digital safety and security risks are widespread in the workplace. Digital safety and security are digital citizenship elements that emphasize protecting and safeguarding information (Ribble, 2021). The result suggests that the employees do not trust company websites. It connotes that the employees believe that their data are transferred to third parties. Per General Data Protection Regulation (GDPR),” ‘the third party means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorized to process personal data” (GENERAL DATA PROTECTION REGULATION (GDPR), n.d.). The data shows that the respondents believed their browsing history and logs were being tracked. The study asserts that web tracking, a widespread phenomenon in the digital environment, poses a growing privacy concern among digital citizens (Ermakova, Fabian, Klimek, & Bender, 2018). In addition, the employees perceived that providing personal information on social media is not safe. This may suggest that digital citizens are aware of several issues on social media such as blackmail, hacking, alteration (Prasansu, 2017), information overload, illegal access of personal information (Majid & Kouser, 2019), addiction (Marcial, Are you a Facebook Addict? Measuring Facebook Addiction at a Philippine University, 2013), narcissism (Marcial, What's on your Mind? Measuring Self-Promotional and Anti-Social Behaviors on Facebook among Tertiary Students, 2015), among others. It can also be argued that workers are cautious of the associated potential risks of social media concerning contact, content, and networking conduct (Mason, 2017). The data shows that the employees perceived that the government could not protect personal information. This can be argued that data privacy laws are not correctly implemented in the government. Also, it can be asserted that working citizens are not satisfied with the government’s effort towards data and information governance, records management, and freedom of information (Shepherd & Flinn, 2010). The result denotes those employees, especially those 29-38 and 59 or older, do not trust that the society is performing responsible netizenship. On the contrary, the employees believe that their fellowmen are responsible citizens in complying with data and privacy law.

The result also suggests that working citizens are advocates against disinformation, misinformation, and mal-information in cyberspace (UNESCO, 2018). The study (Celliers & Hattingh, 2020) concluded that this social media problem is caused by social, cognitive, political, financial, and malicious factors. UNESCO defines “disinformation as information that is false and deliberately created to harm a person, social group, organization or country; misinformation as information that is false but not created with the intention of causing harm; and mal-information as information that is based on reality, used to inflict harm on a person, social group, organization or country” (UNESCO, 2018) The result of this study connotes that the employees are responsible citizens. They are equipped with the necessary skills in digital communication, digital literacy, and digital etiquettes (Ribble, 2021). In addition, the result may mean that the employees have a moderate knowledge, practices, and attitudes towards digital rights and responsibilities like the rights to privacy and freedom of speech responsibly. It can also be claimed that professional and working citizens are equipped with the necessary skills in spotting fake news.

CONCLUSION AND RECOMMENDATIONS

Internet trust is a shared responsibility. It is an emerging issue in any country. Working citizens do not trust that their data and information given to any company website will not be passed on to third parties. The employees believe that their browsing habits are being tracked. Thus, providing personal information on social media is not safe. Employees do not trust that their government is protecting their personal information. Employees from upper-middle-income countries, 29-38 and 59 or older, African, social media spectators and inactive, top managers and contributors do not trust the Internet and social media.

Internet trust is affected by interrelated factors such as demographic, technological, and employment profiles. Age, gender, continent, innovation index, income level, social technologic ladder, internet satisfaction, job position, company form, company role, and company size were significant predictors of Internet trust. Citizens have reasonable trust that their employers, company, government, and compatriots are responsible digital citizens.

An effort should be established among private, government, and non-government organizations to advocate for citizens on the responsible use of social media. There should be an ecosystem to establish aggressive digital citizenship training to achieve empowerment in the workplace (Sánchez , Manzuoli, & Bedoya , 2019). All citizens must deepen their understanding of trust's essence, nature, and psychology on the world wide web (Busch, Colgrove, Li, & Willet, n.d.). Everyone must advocate and practice responsible use of the Internet to have a safe and secure digital economy. The industries must include and initiate their social responsibility to educate netizens about data protection and privacy. Companies must establish a policy on "ensuring protection and privacy of user data, but what about third parties, vendors, and other outside stakeholders" (RIDDLE COMPLIANCE, LLC, n.d.). Most importantly, the government must establish credibility on protecting citizens' personal information.

In today's complexity of the Internet of Things, everyone must escalate their effort to build trust. Research must be rigorously done to achieve a positive reputation for the Internet of Things applications in the workplace (AbdallaAhmed, Hamid, Gani, khan, & Khan, 2019). Research efforts should anchor on the balance between mobility, user-and friendliness, and privacy against web tracking and privacy protection (Ermakova, Fabian, Klimek, & Bender, 2018). A holistic research approach is also suggested, "blending the many consumers, organizational, ethical, and legal concerns that feature in contemporary data privacy questions" (Martin & Murphy, 2017). Disinformation campaigns, interventions to fight misinformation, and research on reclaiming data and information ecology (Pasquetto, et al., 2020) are highly suggested.

Acknowledgment

This research is part of a global study, “Digital Trust and Teamwork,” funded by the European Regional Development Fund, facilitated by Ostfalia University of Applied Sciences. We want to thank the participants during the 5th Management Service Congress on November 24-26, 2021, for their comments and suggestions on the original version of this paper.

References

International Society for Technology in Education (ISTE). (n.d.). DIGITAL CITIZENSHIP IN EDUCATION: Bring Digital Citizenship to the Classroom in Meaningful Ways. (International Society for Technology in Education (ISTE)) Retrieved February 9, 2022 from https://www.iste.org/areas-of-focus/digital-citizenship

AbdallaAhmed, A. I., Hamid, S. H., Gani, A., khan, S., & Khan, M. K. (2019). Trust and reputation for Internet of Things: Fundamentals, taxonomy, and open research challenges. Journal of Network and Computer Applications, 145. doi:https://doi.org/10.1016/j.jnca.2019.102409

APEID-ICT in Education, UNESCO Asia-Pacific Regional Bureau of Education. (2015). Fostering Digital Citizenship Through Safe and Responsible Use of ICT. UNESCO Bangkok. Retrieved February 9, 2022 from https://en.unesco.org/icted/sites/default/files/2019-04/62_fosteing_digital_citizenship_through_safe_and_responsible_use_of_ict.pdf

BBC News. (2019, March 11). World wide web vs internet - what's the difference? BBC News. Retrieved February 4, 2022 from https://www.bbc.co.uk/newsround/47523993#:~:text=The%20world%20wide%20web%2C%20or,emails%20and%20files%20travel%20across.&text=The%20world%20wide%20web%20contains,roads%20like%20houses%20and%20shops.

Busch, k., Colgrove, C., Li, F., & Willet, N. (n.d.). Psychology of Trust on the Internet. From https://cs.stanford.edu/people/eroberts/cs201/projects/2010-11/PsychologyOfTrust/

Celliers, M., & Hattingh, M. (2020). A Systematic Review on Fake News Themes Reported in Literature. Lecture Notes in Computer Science, 223–234. doi:https://doi.org/10.1007/978-3-030-45002-1_19

Choudhury, N. (2014). World Wide Web and Its Journey from Web 1.0 to Web 4.0. International Journal of Computer Science and Information Technologies, 5(6), 8096-8100. From http://ijcsit.com/docs/Volume%205/vol5issue06/ijcsit20140506265.pdf

Conrad, K., & Combs, J. (2017). Trust: The Foundation for Serving Citizens in a Digital World. Retrieved February 9, 2022 from https://www.accenture.com/_acnmedia/PDF-115/Accenture-Citizen-Trust-POV.pdf

Diffen. (2012). Internet vs. World Wide Web. (Diffen) Retrieved February 4, 2022 from https://www.diffen.com/difference/Internet_vs_World_Wide_Web

Ermakova, T., Fabian, B., Klimek, K., & Bender, B. (2018). Web Tracking – A Literature Review on the State of Research. The Hawaii International Conference on System Sciences (HICSS 51). doi:10.24251/HICSS.2018.596

FutureLearn. (2021, September 3). What is digital citizenship? – A guide for teachers. (FutureLearn) Retrieved February 9, 2022 from https://www.futurelearn.com/info/blog/what-is-digital-citizenship-teacher-guide

GENERAL DATA PROTECTION REGULATION (GDPR). (n.d.). (Intersoft Consulting) Retrieved https://gdpr-info.eu/art-4-gdpr/

Google Arts and Culture. (n.d.). The World Wide Web: The Invention That Connected The World. (Google Arts and Culture) Retrieved February 4, 2022 from https://artsandculture.google.com/theme/the-world-wide-web-the-invention-that-connected-the-world/eAJS4WcKh7UBIQ?hl=en

Lazic, M. (2021, January 4). 39 Worrying Cyber Crime Statistics [Updated for 2022]. (Legal Jobs) Retrieved February 4, 2022 from https://legaljobs.io/blog/cyber-crime-statistics/

Majid, I., & Kouser, S. (2019). Social media and security: how to ensure safe social networking. International Journal of Humanities and Education Research, 1(1), 36-38. From https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3804420

Marcial, D. E. (2013). Are you a Facebook Addict? Measuring Facebook Addiction at a Philippine University. Education, Research and Innovation III, 66, 12-15. From : https://www.researchgate.net/publication/285678122

Marcial, D. E. (2015). What's on your Mind? Measuring Self-Promotional and Anti-Social Behaviors on Facebook among Tertiary Students. Information Technologies and Learning Tools, 48(4), 199-208. doi:https://doi.org/10.33407/itlt.v48i4.1272

Marcial, D. E., & Launer, M. (2019). Towards the Measure of Digital Trust in the Workplace: A Proposed Framework. 3(12), 1-7. doi:10.5281/zenodo.3595295

Marcial, D. E., & Launer, M. A. (2021). Test-retest Reliability and Internal Consistency of the Survey Questionnaire on Digital Trust in the Workplace. 64(2), 4369-4381. From https://solidstatetechnology.us/index.php/JSST/article/view/10225?fbclid=IwAR2L5ztiRa-RtDQER7vuXS8v6A46_nGu59gUYSef5hXyW24uh16nNgBL5iw

Marcinek, A. (2014, October 22). Digital Citizenship: Developing a Culture of Trust and Transparency. (Edutopia) Retrieved February 9, 2022 from https://www.edutopia.org/blog/digital-citizenship-culture-trust-transparency-andrew-marcinek

Martin, K. D., & Murphy, P. E. (2017). The Role of Data Privacy in Marketing. Journal of the Academy of Marketing Science, 45(2), 135–155. doi:10.1007/s11747-016-0495-4

Mason, M. (2017). The use of the internet and social media by young people. Effective Practice in Youth Justice, 1-18.

Pasquetto, I. V., Swire-Thompson, B., Amazeen, M. A., Benevenuto, F., Brashier, N. M., Bond, R. M., . . . Yang, K.-C. (2020, December 9). Tackling misinformation: What researchers could do with social media data. Harvard Kennedy School Misinformation Review. From https://misinforeview.hks.harvard.edu/article/tackling-misinformation-what-researchers-could-do-with-social-media-data/

Prasansu, H. (2017). Social Media: Security and Privacy. International Journal of Scientific & Engineering Research, 8(11), 527-529. From https://www.ijser.org/researchpaper/Social-Media-Security-and-Privacy.pdf

Ribble, M. (2021, July 26). Essential Elements of Digital Citizenship. Retrieved March 1, 2022 from International Society for Technology in Education: https://www.iste.org/explore/digital-citizenship/essential-elements-digital-citizenship

Richardson, J., & Milovidov, E. (2019). Digital Citizenship Education Handbook. GCED Clearinghouse. From https://gcedclearinghouse.org/resources/digital-citizenship-education-handbook

RIDDLE COMPLIANCE, LLC. (n.d.). GDPR AND THIRD PARTIES: WHAT COMPANIES NEED TO KNOW. Retrieved March 1, 2022 from https://www.riddlecompliance.com/blog/gdpr-and-third-parties-what-companies-need-to-know

Sánchez , A. V., Manzuoli, H. C., & Bedoya , D. E. (2019). Digital Citizenship: A Theoretical Review of the Concept and Trends. The Turkish Online Journal of Educational Technology, 18(2), 10-18. From http://www.tojet.net/articles/v18i2/1822.pdf

Schwab, K. (2016, January 14). Fourth Industrial Revolution. World Economic Forum. From https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/

Shepherd, E., & Flinn, A. (2010). Information governance, records management and freedom of information: a study of local government authorities in England. Government Information Quarterly, 27(4), 337-345. doi:10.1016/j.giq.2010.02.008

Solanki, M. R., & Dongaonkar, A. (2016). A Journey of Human Comfort: Web 1.0 to Web 4.0. International Journal of Research and Scientific Innovation, 78(9), 75. From https://www.rsisinternational.org/IJRSI/Issue31/75-78.pdf

The Editors of Encyclopaedia Britannica. (2019, November 27). World Wide Web. (The Editors of Encyclopaedia Britannica) Retrieved February 4, 2022 from https://www.britannica.com/topic/World-Wide-Web

UNCTAD. (2019, June). Survey says people don't trust the Internet, what needs to change? (United Nations Conference on Trade and Development) Retrieved February 9, 2022 from https://unctad.org/news/survey-says-people-dont-trust-internet-what-needs-change

UNESCO. (2018). 'Fake News' and Disinformation: A Handbook for Journalism Education and Training. UNESCO. Retrieved March 2, 2022 from https://en.unesco.org/fightfakenews