World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:15, No:9, 2021

User's Susceptibility Factors to Malware Attacks: A Systemic Literature Review

Awad A. Younis, Elise Stronberg, Shifa Noor

Open Science Index, Computer and Information Engineering Vol:15, No:9, 2021 publications.waset.org/10012256.pdf

***Abstract*—**Users' susceptibility to malware attacks have been noticed in the past few years. Investigating the factors that make a user vulnerable to those attacks is critical because they can be utilized to set up proactive strategies such as awareness and education to mitigate the impacts of those attacks. Demographic, behavioral, and cultural vulnerabilities are the main factors that make users susceptible to malware attacks. It is challenging, however, to draw more general conclusions based on those factors due to the varieties in the type of users and different types of malware. Therefore, we conducted a systematic literature review (SLR) of the existing research for user susceptibility factors to malware attacks. The results showed that all demographic factors are consistently associated with malware infection regardless of the users' type except for age and gender. Besides, the association of culture and personality factors with malware infection is consistent in most of the selected studies and for all types of users. Moreover, malware infection varies based on age, geographic location, and host types. We propose that future studies should carefully take into consideration the type of users because different users may be exposed to different threats or targeted based on their user domains' characteristics. Additionally, as different types of malware use different tactics to trick users, taking the malware types into consideration is important.

***Keywords*—**Cybersecurity, malware, users, demographics, personality, culture, systematic literature review

I. Introduction

MALICIOUS software, also known as malware, has recently become a critical security threat to users [1]. Many researchers consider users, just as much as technology, to be the weakest link in the cybersecurity domain [2]-[4]. Both the magnitude and impact of the malware infection are influenced by the actions (direct or indirect) of users. These actions may occur immediately before malware infection such as opening an email attachment or visiting a malicious web or may occur over time such as not updating the system or voluntarily installing antimalware software. Therefore, examining the factors that make a user vulnerable to these attacks is important because it can be used to develop preventive measures, such as awareness and education, to help reduce the effects of these attacks or providing additional defense for those most at risk [5].

There exist individual studies that investigated demographic, behavioral, and situational factors that make a user susceptible to malware attacks [5], [13]-[30]. However, since there are many different types of end users (academia, residents, employees, etc.) and types of malware (adware, virus, cracks, hack, exploit, rogue malware, infostealer, ransomware, etc.), it has been difficult to draw more general conclusions from individual studies. Generalizing the results and risk of susceptibility factors to malware attacks from one user type to another could be problematic, because a different type of users may be exposed to different threats or be targeted based on their user domains' characteristics. Considering the type of malware is important, because different malware types are known to use different tactics, (e.g., differences in emotional processing; differences in frequency and type of computer usage; and risk perceptions), to trick users into downloading a file or clicking on a link inside an email. To the best of our knowledge, this is the only SLR on user's susceptibility factors to malware attacks.

We have developed detailed assessment criteria reflecting our research questions. Our search strategy included an automatic search of three digital libraries and snowballing. Using the 19 final selected studies, we extracted the needed information from each article to answer the research questions by using a study profile card. We then synthesized the content from the 19 profile cards using a table

as a visualization technique. To simplify the analysis, we have categorized the identified susceptibility factors into three categories: demographics (gender, age, education/training, experience, etc.), personality (individual's cognitive process, attitudes, and behavioral outcomes), and culture (national culture and organizational culture) using the categories of human factors in cybersecurity as discussed in [6], [7]. Additionally, we compared the extracted content based on the type of users, research method and sample size, and theoretical framework.

The rest of the paper is organized as follows. Section II describes the research methodology, including the research questions and data extraction strategy. Section III presents the results, whereas Section IV discusses those results and the limitation. Section V presents the concluding remarks.

II. Research Methodology

The methodology adopted for the extraction of user's susceptibility factors to malware attacks is a SLR. By following the steps presented by [8] (planning, conducting, and documenting the review), we collected and analyzed the literature. Our motivation for an SLR is driven by the need to draw more general conclusions from individual studies. That

A. A. Y. is with the Northern Kentucky University, Highland Heights, KY 41099 USA (corresponding author, phone: 859-572-7922; e-mail: mussaa1@nku.edu).

E. S. and S. N. are students with the Northern Kentucky University, Highland Heights, KY 41099 USA. (e-mail: strombergel@mymail.nku.edu, noors1@mymail.nku.edu).

Open Science Index, Computer and Information Engineering Vol:15, No:9, 2021 publications.waset.org/10012256.pdf

could help in designing, developing, and customizing awareness and personalized educational resources and training based on a personal level of risk, and hence mitigate the impacts of the malware attacks. We searched for comparative SLR in the following digital libraries: Google Scholar as well as the Northern Kentucky University library discovery search, which includes the following digital libraries: ACM, Applied Science & Technology Full Text, Career & Technical Education Database, and JSTOR Security Studies. None of the mentioned digital libraries contained an SLR about user's susceptibility factors to malware attacks.

A. Research Questions

The main objective of this study is to identify users' susceptibility factors to malware attacks. Thus, we reviewed the selected literature to answer the following research questions:

- RQ1: What susceptibility factors are associated with a user falling for malware attacks?
- RQ2: How do the susceptibility factors vary based on the type of malware?

The purpose of RQ1 is to identify the main susceptibility factors that are associated with a user falling for malware attacks. That is important for employers who may need to design and develop personalized awareness and educational resources and training; and for providing additional defense for those who most at risk, as requiring additional defenses often involves imposing additional usability costs on users [9], [10]. The purpose of RQ2 is to identify the susceptibility factors that vary based on the type of malware. This is important because different malware types are known to use different tactics (e.g., differences in emotional processing; differences in frequency and type of computer usage; and risk perceptions) to trick users into downloading a file or clicking on a link inside an email.

B. Search Process

Our search process included an automatic search of digital libraries using search strings as well as backward snowballing. The search strings were constructed based on the guidelines provided in [8]. We broke down the research questions and extracted the major terms (keywords and their synonyms), and then we identified the keywords and subject terms from relevant papers' titles, abstracts, and keywords. It should be noted that we conducted pilot searches so to refine the search string. The major keywords, subject terms, and their synonyms were concatenated with the help of "OR" and "AND" operators to construct the following search strings:

- (*user* OR *user* factor*) AND
- (risk* OR susceptibility) AND
- (malware OR ransomware)

Using the constructed search strings, we first obtained studies from the following digital libraries: Google Scholar, as well as the Northern Kentucky University (NKU) library discovery search, that, is ACM and ScienceDirect. The search for this study was not limited by the year of publication. Table I presents the search result performed in December 2020 using the three digital libraries. The search results were ordered by relevance and cut to top 1000 for Google Scholar, and to top 2000 for ACM and ScienceDirect.

TABLE I
STRINGS SEARCH RESULTS USING DIGITAL LIBRARIES

	Google Scholar	ACM	ScienceDirect
Search Results	48,500	2490	4620
Search Results Ordered by Relevance and Cut to Top	1000	2000	2000

C. Inclusion and Exclusion Criteria

We proceeded to filter the search results in Table I in several steps, as shown in the inclusion and exclusion criteria subsection. Table II shows the summarized inclusion and exclusion criteria. We were interested in the work published at any time before November 2020 that presents a contribution to the area of users' risk factors to malware attacks. We have noticed that many search results focused on phishing and cybercrime topics, and that led us to the last two exclusion criteria.

TABLE II
INCLUSION AND EXCLUSION CRITERIA

Inclusion criteria	Exclusion criteria
1. Primary studies (peer-reviewed journal or conference papers).	1. Studies that are: • written in any language other than the English language, • we had neither digital nor physical access to the full text, • unavailable through the search engine. • appeared more than once or duplicate data sets and synthesis of the research.
2. Studies that address user's risk or susceptibility factors and malware attacks.	2. Studies that focus on: • organizational or defender factors with minimal overlap with user's susceptibility or risk factors,
3. Studies that relate to malware attacks (e.g., malware-based phishing or malware email-based attacks) and users' factors in cybersecurity or cybercrime.	• phishing or email-based attacks with minimal overlap with user's susceptibility or risk factors or vice versa • developing or applying user's vulnerabilities mitigation techniques, • malware detection techniques, • trends.

Using the criteria in Table II, the following three filtering processes were carried out to ensure that only highly relevant studies were selected. After applying those three filters manually, the number of search results decreased, as shown in Table III. After applying filtering 1, the number of search results considerably decreased to 334. When applying the second filtering to 334 remaining studies, the number of search results decreased to 31. Finally, after applying filtering 3, the number of search results decreased to 18.

- Filtering 1: Applying the inclusion and exclusion criteria to titles and keywords.
- Filtering 2: Applying the inclusion and exclusion criteria to abstract and conclusions.
- Filtering 3: Applying the inclusion and exclusion criteria to the full text.

Next, we performed a backward snowballing search method [11]. This search method involves applying Filtering 4, as shown below on the referenced work of a final set of studies.

- Filtering 4: Applying the inclusion and exclusion criteria to the entire papers obtained from snowballing.

Open Science Index, Computer and Information Engineering Vol:15, No:9, 2021 publications.waset.org/10012256.pdf

In our case, snowballing was performed on 18 papers. After applying filtering 4 on the selected nine papers, three papers have been chosen. The number of search results increased to 19, as shown in Table III. Those 19 studies were selected to be included in this SLR.

TABLE III
SEARCH METHOD USED IN THE STUDY

Search Method	Search Results	Filters	Filters Results	Included Studies
1.Digital Libraries:	5000	Filtering 1	334	19
• Google Scholar		Filtering 2	31	
• ACM				
• ScienceDirect		Filtering 3	16	
2. Snowballing	9	Filtering 4	3	

D. Data Extraction

Using the 19 final selected studies, we extracted the needed information from each article to answer the research questions by using a study profile card recommended by [12]. Table IV shows an example of the attribute names assigned for each study. Each study profile card covers a summary of: 1) author, year, title, and publication type; 2) research objective; 2) main findings; 4) research methodology; 5) susceptibility factor; 6) user type; 7) malware type, and 8) geographical region. The extracted data was stored in spreadsheets to use in the data synthesis process.

TABLE IV
EXAMPLE OF STUDY PROFILE CARD

[#] Author / Year/ Title/ Publication Type	Research Objective
#2, Lévesque et al., 2013, A Clinical Study of Risk Factors Related to Malware Infections, Conference paper.	To examine the interactions between users, antivirus (anti-malware) software, and malware as they occur on deployed systems. Summary of Findings • Results show that while user behavior is significant, user characteristics such as age or gender are not significant risk factors. • Websites such as sports and Internet infrastructure being associated with a higher rate of infection while websites containing pornography and illegal/questionable content were less so. • Computer expertise is a weak factor increasing the risk of infection.
Research Method: Experiment (n = 50) Theoretical Framework: Ecological validity and clinical trial Susceptibility Factor: Behavior, age, gender, and computer expertise User Type: Students and employees Malware Type: Trojan, Adware, Virus, Worm, Others Geographical Region: Canada	

E. Data Synthesis

We synthesized the content from the 19 profile cards using a table as a visualization technique, as shown in Table V. The specific studies that are referenced in the sections and subsections below are indicated by the numerical order specified and represented by a #.

III. RESULTS

In this section, we first overview the selected studies and then present the answers to the research questions based on the summary outlined in Table V.

A. Overview of User's Susceptibility Factors to Malware Attacks Studies

Fig. 1 shows a timeline of the 19 studies included in this SLR (10 conference papers and nine journal articles). As can be seen, the interest in user's susceptibility factors to malware attacks looks to be constant, with an average of almost two (1.68) publications per year. There is a progression of publications starting 2008 and three peaks are reached in 2011, and the period of 2013 until 2014 and 2016 until 2018. As also shown, the number of publications decreased during 2012, 2015, and 2019.

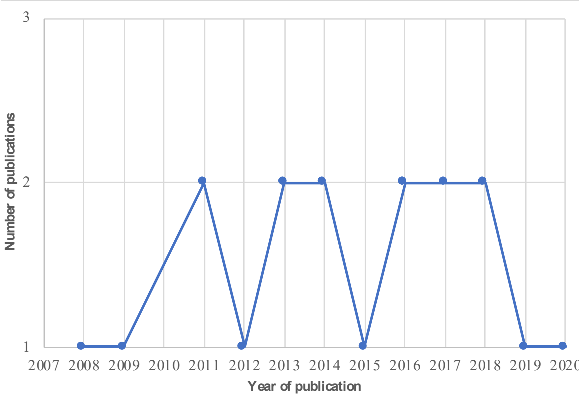

Fig. 1 Year of publication for the selected studies

Fig. 2 shows that a case study is the most used research method followed by a survey. This could be due to the adoption of epidemiology as a framework, which commonly uses the case study as the study design. Besides, case studies are comparatively quick, inexpensive, and easy [31].

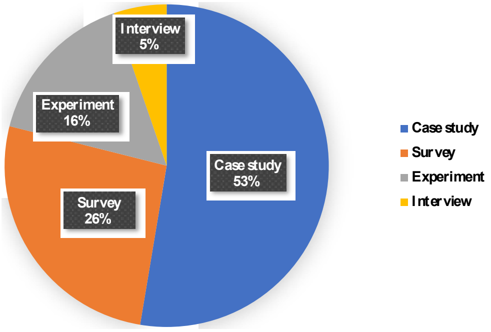

Fig. 2 Research Method Used

Open Science Index, Computer and Information Engineering Vol:15, No:9, 2021 publications.waset.org/10012256.pdf

TABLE V
SUMMARY OF THE SELECTED STUDIES

Study #	Author	Year	Type of Publication	Susceptibility Factors	User Type	Malware Type	Research Method	Theoretical Framework	Geographical Region
1	Carlinet et al. [13]	2008	Conference paper	Behavior: Using peer-to-peer applications; Using Windows; Surfing the web; Using streaming applications; Using chat applications	Orange ADSL customers	Viruses and worms	Case study (n = 6675)	Epidemiology,	France
2	Bossler and Holt [14]	2009	Journal article	a) Behavior: on-line activities, guardianship: antivirus programs and critical operating system updates, opening emails from unknowns, using strong and regularly changed password, and gaining knowledge of computer technology b) employment status, gander, age, computer skills	College students	Viruses, worms and trojan horse	Survey (n = 788)	Routine activities framework	USA (Southeastern University)
3	Ngo and Paternoste [15]	2011	Journal article	Age, gender, race, material status, employment	College students	Virus, spyware,	Survey (n = 295)	General theory of crime and the lifestyle/ routine activities framework	USA (Southeastern University)
4	Maier et al. [16]	2011	Conference paper	a) Behavior: security hygiene (anti-virus and OS software updates) AND risky behavior (accessing blacklisted URLs) b) Geographical location	Residential users (DSL customers, users of a community network, and dormitory users at a large university)	Family: Zlob, Conficker, and Zeus	Case study (n = 28000)	Hygiene framework	Europe, USA, India
5	Lee [17]	2012	Conference paper	Area of expertise,	Researchers in academic institutions	Trojan, and others	Case control study (n = 370)	Epidemiology	US, UK, and others
6	Lévesque et al. [18]	2013	Conference paper	a) Behavior: used browser, total number of applications installed, total number of websites visited, categories of websites visited. b) Age, gender, Status, Field of study, Computer Expertise,	Students and employees	Trojan, Adware, Virus, Worm, Others	Experiment (n = 50)	Ecological validity and clinical trial	Canada
7	Holt and Bossler [19]	2013	Journal article.	a) Gender, age, skills level b) Behavior: Shopping, Video games, Email, Chatrooms, Ownership, Connectivity, Downloading, Instant messaging, Computer Deviance, Antivirus, Software firewall, Spybot, and Hardware firewall	Students and faculty at a university	Trojan, Adware, Virus, Worm, Others	Survey, (n = 5,384)	Routine Activities framework	USA (Southeastern University)
8	Yen et. al. [20]	2014	Conference paper	a) Level of technical skills, job type, technical expertise, country b) Behavior: browsing behavior (categories of web sites visited, web traffic volume), using VPN	Employees	Exploit, Ransom, AdClicker, ProcKill, Keylog, Dropper, FakeAV, Downloader, BackDoor.	Case Study (n = 62,884, 9625)	Epidemiology	USA, India, China, Egypt, Brazil, Germany, Israel, UK, and S. Korea
9	Canali et al. [21]	2014	Conference paper	a) Behavior: How Much a User Surfs the Web, In Which Period of the Day a User is More Active, How Diversified is the Set of Websites Visited by a User, Which Website Categories the User is Mostly Interested in, Computer Type, How Popular are the Websites Visited by the User, and How Stable is the Set of Visited Pages. b) Geographical location	Symantec Antivirus users	All types of malware provided by the Malware Domain List	Case study (n = 100000)	User Profiling framework	US, UK, JP, CA , AU , DE , FR, NL, ES, SE, IT, BE, NO
10	Thonnard et al. [22]	2015	Conference paper	a) Job Type, Job level, b) Geographical location,	Employees	Trojans and worms and	Case control studies (n =	Epidemiology and profiling	USA, Australia, India, China,

Open Science Index, Computer and Information Engineering Vol:15, No:9, 2021 publications.waset.org/10012256.pdf

Study #	Author	Year	Type of Publication	Susceptibility Factors	User Type	Malware Type	Research Method	Theoretical Framework	Geographical Region
				organizational classification codes, and the organizational size,		occasionally a virus	16181)		Brazil, Europe
11	Jansen and Leukfeldt [23]	2016	Journal article	Behavior: PMT: response efficacy, self-efficacy and response costs; experience with online banking, use of protective measures; RA: Value(large sums of money in bank account), Visibility (downloading and spending time on social media) and Accessibility (weaknesses in software that can be used by fraudsters to attack customers)	Bank customers	Not specified (any type of malware)	Semi-structured Interview (n = 30)	The routine activity approach and protection motivation theory	Netherlands
12	Neupane et al. [24]	2016	Journal article	Behavior: personality traits (impulsivity) and security behavior: malware wrongs, legitimacy of websites	University students	Not specified (any type of malware)	Experiment (n = 25)	Neuroscience	USA
13	Levesque et al. [25]	2016	Journal article.	a) Geographic locations b) Economy, education, c) Use of technology, global cybersecurity index, and use of antivirus	Country residents (Computer and internet users)	Not specified (any type of malware)	Case study (n = 100+ M)	Ecological studies	Multi-country (names not specified)
14	Lévesque et al. [26]	2017	Conference paper	Gender, age	Microsoft services users (Outlook, Skype, OneDrive)	Adware, virus, cracks, hack, exploit, rogue malware, infostealer, ransomware, bot, and rootkit	Case-control study (3,019, 671)	Epidemiology	North America, Europe, South and Central America, Australia, Asia and Pacific, Africa and Middle East
15	Ovelgonne et al. [27]	2017	Journal article	a) Behavior: the number of low-prevalence binaries downloaded by the users, number of unique binaries on users' machines, number of unsigned binaries on the users' machines, and number of binaries downloaded by users b) Type of professions (gamer, pro, SW-dev, other describing gamers, professionals (other than software developers), software developers, and all others)	Symantec's Norton Anti-Virus users (gamers, professionals, software developers, and others)	viruses, worms, bots, trojans, etc.	Case study (n = 1.6M)	Analytical model	20 countries (names not specified)
16	Levesque et al. [28]	2018	Journal article	a) Gender, age, employment status, field of expertise, computer expertise b) Behavior: System activity, Applications installed, Outdated applications, Connection time, Hosts contacted, Default web browser, Web pages visited, Files downloaded, and P2P activity	Students	Trojan, Adware, Virus, Worm, Others	Experiment (n = 100)	Ecological and Clinical trial	Canada
17	Blythe and Coventry [29]	2018	Journal article.	Behavior: security behavior (use of anti-malware software to scan USB sticks (‘anti-malware software’), avoiding links in suspicious emails (‘email security’) and installing software updates when prompted (‘software updates’)	Employees	Not specified (any type of malware)	Survey (n = 526)	Protection Motivation Theory (PMT)	UK
18	Simoiu et al. [5]	2019	Conference paper	Behavior: security habits (use two-step authentication, computer password-protected for login, downloaded malicious applications, backup your personal files to an external hard drive or a cloud-based, download files from online torrent sites such as the Pirate Bay, ExtraTorrent, or TorrentZ2) and previous experience with online scams	U.S. adults	Ransomware	Survey (n = 1180)	Analytical model	USA

Open Science Index, Computer and Information Engineering Vol:15, No:9, 2021 publications.waset.org/10012256.pdf

Study #	Author	Year	Type of Publication	Susceptibility Factors	User Type	Malware Type	Research Method	Theoretical Framework	Geographical Region
19	Simoiu et al. [30]	2020	Conference paper	a) Age, country b) Behavior: security posture, prior risk exposure, type of device, email activity c) Geographical location	Gmail users	Emotet family, botnet's	Case study (17 M)	Analytical model	United States, Japan, India, United Kingdom, Brazil, Spain, France, Canada, Australia, Indonesia

As can be seen from Fig. 3, researchers have adopted a variety of theoretical frameworks including: routine activity, protection motivation theory; neuroscience; ecology; epidemiology; analytical models; general theory of crime; hygiene; and user profiling. Epidemiology theory is the most adopted and used technique and it has been used by different researchers from 2008 to 2017. Starting from 2017 to 2020, the analytical model (data driven approach) has been the most adopted and used framework whereas hygiene and the general theory of crime have not been used for almost 10 years.

Looking at the population samples used to identify the susceptibility factors for malware attacks, students are the most sample used by serval studies, as shown in Fig. 4. This could be due to the facility of recruitment, lower cost of administration, and assumed lower response bias [32]. However, generalizing from student samples to the general public has been found problematic when personal and attitudinal variables are utilized, as students vary mostly randomly from the general public across countries and variables [33]. Looking at the georgical location in the selected studies, we noticed that students are used as a sample only in North America (four studies in the USA, and two in Canada).

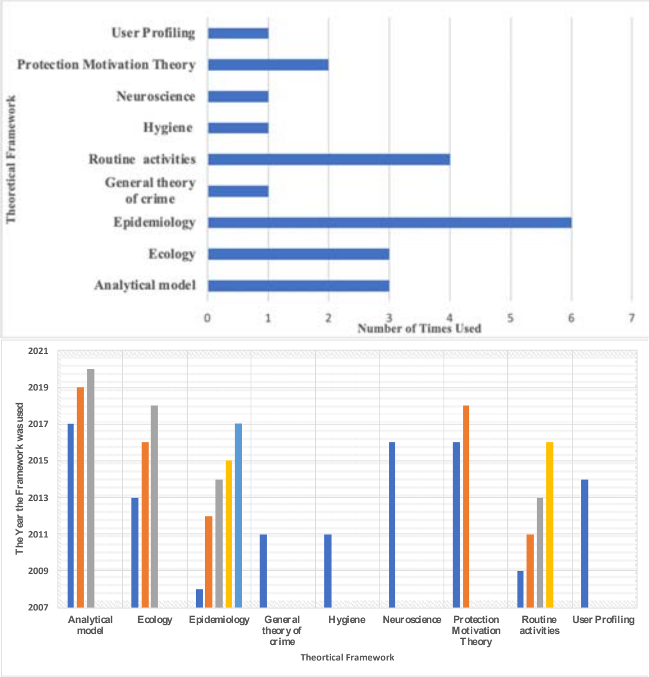

Fig. 3 Theoretical Frameworks

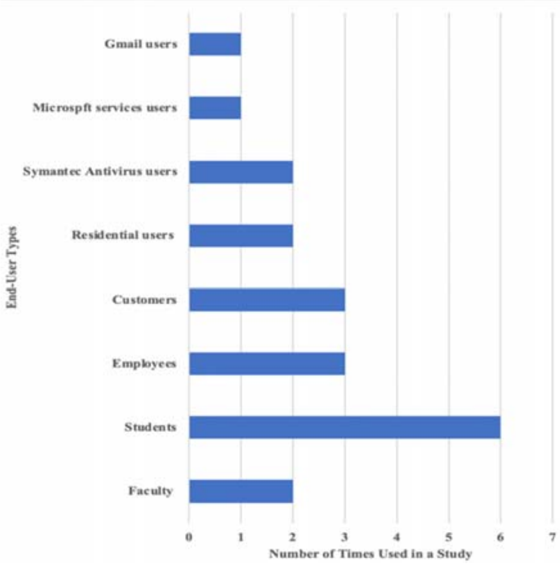

Fig. 4 Population Samples

B. RQ1: What Susceptibility Factors Are Associated with a User Falling for Malware Attacks?

The purpose of RQ1 is to identify the susceptibility factors that are associated with an user falling for malware attacks. There are 15 susceptibility factors identified by the selected 19 studies including: Gender, Age, Computer expertise, Field of expertise/study, Level of technical skills, Level of education, Type of professions, Job type and level, Employment status, Level of economy, Country, Geographical location, Organizational classification, Organizational size, and Behavior. We have noticed that the studies that investigated the behavior factor have considered varieties of subfactors. Each of the following points represents the group of subfactors considered by each study (15 out of 19 studies):

- Using peer-to-peer applications; using windows; using streaming applications; using chat applications.
- On-line activities; using antivirus programs; installing critical operating system updates; opening emails from unknowns; using strong and regularly changed password.
- Security hygiene (anti-virus and OS software updates); Risky behavior (accessing blacklisted URLs).
- Used browser; total number of applications installed; total number of websites visited; categories of websites visited.
- Shopping; video games; email; chatrooms; ownership; connectivity; downloading; instant messaging; spybot; hardware firewall.
- Browsing behavior (categories of web sites visited, web traffic volume)
- Using a VPN.

- Number of times the user surface the web; period of the day a user is more active; the degree of diversifying the set of websites visited are; categories of website the user is mostly interested in; popularity of websites visited by the user; stability of the set of visited pages.
- Response efficacy, self-efficacy and response costs; value (large sums of money in bank account); visibility (downloading and spending time on social media); accessibility (weaknesses in software that can be used by fraudsters to attack customers).
- Personality traits (impulsivity) and security behavior (malware wrongs, legitimacy of websites).
- Use of technology; use of antivirus.
- Number of unique binaries on users' machines; number of unsigned binaries on the users' machines; number of binaries downloaded by users; travel by a host machine.
- System activity; applications installed; outdated applications; connection time; hosts contacted; default web browser; web pages visited; files downloaded; P2P activity.
- Use of anti-malware software to scan USB sticks; avoiding links in suspicious emails; update software.
- Use two-step authentication; computer password-protected for login; downloaded malicious applications; backup your personal files to an external hard drive or a cloud.
- Security posture; prior risk exposure; type of device; email activity.

Open Science Index, Computer and Information Engineering Vol:15, No:9, 2021 publications.waset.org/10012256.pdf

TABLE VI
SUSCEPTIBILITY FACTORS

Study #	Author	Year	Categories of Susceptibility Factors			User Type	Research Method	Theoretical Framework
			Demographics	Personality	Culture			
2	Bossler and Holt [6]	2009	X	X		College students	Case study (n = 6675)	Epidemiology,
3	Ngo and Paternoste [7]	2011	X			College students	Survey (n = 788)	Routine activities framework
12	Neupane et al. [16]	2016		X		University students	Case control study (n = 370)	Epidemiology
16	Levesque et al. [20]	2018	X	X		Students	Experiment (n = 50)	Ecological validity and clinical trial
7	Holt and Bossler [11]	2013	X	X		Students and faculty	Case study (n = 28000)	Hygiene framework
5	Lee [9]	2012	X			Researchers	Survey (n = 295)	General theory of crime and the lifestyle/routine activities framework
1	Carlinet et al. [5]	2008		X		ADSL customers	Survey, (n = 5,384)	Routine Activities framework
4	Maier et al. [8]	2011		X	X	Residential users	Case Study (n = 62,884, 9625)	Epidemiology
11	Jansen and Leukfeldt [15]	2016		X		Bank customers	Case study (n = 100000)	User Profiling framework
13	Levesque et al. [17]	2016	X	X	X	Country residents	Case control studies (n = 16181)	Epidemiology and profiling
18	Simoiu et al. [22]	2019		X		U.S. residents	Case study (17 M)	Analytical model
8	Yen et. al. [12]	2014	X	X		Employees (enterprise)	Semi-structured Interview (n = 30)	The routine activity approach and protection motivation theory
10	Thonnard et al. [14]	2015	X		X	Employees (number of enterprises)	Experiment (n = 25)	Neuroscience
17	Blythe and Coventry [21]	2018		X		Employees (enterprises)	Case study (n = 100+ M)	Ecological studies
9	Canali et al. [13]	2014		X	X	Symantec Antivirus users	Case-control study (3,019, 671)	Epidemiology
14	Lévesque et al. [18]	2017	X			Microsoft services users	Case study (n = 1.6M)	Analytical model
15	Ovelgonne et. al. [19]	2017	X	X		Symantec's users	Experiment (n = 100)	Ecological and Clinical trial
19	Simoiu et. al. [23]	2020	X	X	X	Gmail users	Survey (n = 526)	Protection Motivation Theory (PMT)
6	Lévesque et al. [10]	2013	X	X		Students and employees	Survey (n = 1180)	Analytical model

We then categorized the identified susceptibility factors using the categories of human factors in cybersecurity as discussed in [6], [7] to simplify their analysis. As shown in Table VI, the susceptibility factors category of the selected studies fit into three broad categories.

- Demographics: Consist of the size, structure, and distribution of a population (e.g., gender, age, education/ training, experience, etc.).
- Personality: An individual's cognitive process, attitudes, and behavioral outcomes.

Open Science Index, Computer and Information Engineering Vol:15, No:9, 2021 publications.waset.org/10012256.pdf

- Culture: Consists of two categories national and organizational culture: National Culture refers to a culture-specific to a group of people within a specific geographical location; and Organizational Culture refers to a culture that is associated with a particular business and/or organization.

It should be noted that we consider workload, stress, and vigilance, which are identified as human performance factors by [7], as part of the personality. As it can be seen from Table VII, during the period 2016-2020, there was more research conducted in personality. Besides, less research in culture compared to demographics and personality.

The results and risk factors may vary based on the type of users, (e.g., home-user, industry, government, academia, etc.), because different types of users may be exposed to different computer threats or be targeted based on their user domains' characteristics. This should be taken into consideration when analyzing and comparing the susceptibility factors. Thus, we compared the results of the studies based on the type of users. Based on the collected data, we classified users into academia, residents, employees, serveries' (email, antivirus, etc.) users, and employees and students. As shown in Table VI, each susceptibility factor demission will be compared based on the above-mentioned users' type.

i. Demographics

Demography characteristics consist of the size, structure, and distribution of a population [34]. To help society plan for and cope with the growing danger presented by cybersecurity, demographic characteristics are a key factor. The selected studies considered the following demography characteristics: age, gender; expertise, education, and employment status, and level of the economy. These characteristics are presented based on the users' type as follows:

Academia: Age and Gender. In study #3, the authors showed that the effect of age was identified as a significant predictor for computer virus infection. Moreover, in study #16, the results suggested that age may be a contributing factor associated with the risk of malware attack. However, based on study #2, age was not found to be a significant predictor of self-reported data loss from malware infection. It should be noted that the sample size for study #2 was the largest: 6675, whereas study #3 was 788 and study #16 was 50. In studies #2 and #7, the authors found that gender is one of the risk factors and they pointed out that being female increases the odds of data loss compared to a male even after controlling for legitimate and illegal computer behaviors. However, based on the results from study #3, the gender was not found significant. It should be noted that study #7 had the largest sample size: 28000, whereas study #2 and study #3 were 6675 and 788, respectively.

Expertise and Education: The results in study #5 showed that an individual's area of expertise (not in the areas of technology, science, or engineering) led to them becoming of interest to attackers and becoming subject to targeted attacks. In study #7, the results showed that having a high level of computer skill is considered as personal guardianship against malware infection. However, in study #16, the results showed that the field of expertise had no statistically significant effect on the risk of malware attack. Besides, the same study showed that having a high level of expertise increases the risk of malware attacks. It should be noted that study #5 and #7 had the largest sample sizes: 28000 and 295 respectively, whereas study #16 sample size was 50.

Employment Status: In study #2, the results showed that employment status was correlated with the victimization of malware attack, however, study #16 shows that the employment status were not significant correlates of malware attacks. It should be noted that the study #2 sample size was 6675.

Residents: Expertise and Education. In study #13, the authors found that education was more consistently associated with reduced malware infection rates.

Level of Economy*:* In study #13, the authors found that the level of the economy, (measured using GDP), was not a significant factor of malware infections.

Employees: Expertise and Education. In study #8, the authors showed that the likelihood of encountering malware increases with job type and level and technical proficiency. In study #10, both job type and level were investigated, the result showed that directors and managers were at higher risk of being targeted than individual contributors.

Serveries Users: Age and Gender. In study #14, the results showed that both age and gender are significant contributing factors for malware encounters. Besides, men, (particularly young men), were found to be more susceptible to malware attacks than women, and users of younger age were found to be more at risk than older users. It should be noted that the authors also pointed out that the effect of age and gender is not constant across different types of malware. They found that women were slightly more susceptible to encounter adware, and older users were more susceptible to rogue malware and ransomware. In study #19, the authors also found age to be one of the high-risk factors of being targeted by malware attacks. The results showed that people over 65 years old face 1.50 times higher risk compared to 18–24-year-olds who face the lowest risk. Their reasoning for this observation was that older people are more susceptible to deception and coercion, as well as older users may have larger online footprints which make discovering their accounts easier.

Expertise and Education: In study #15, the authors found that a high level of expertise increases the risk of exposure to malware attacks.

Students and Employees: Age and Gender. In study #6, the authors found no significant differences based on gender or age.

ii. Culture Characteristics

Scholars have proposed that the culture concept should be broken up into more manageable categories and parts namely national and organizational [7]. The selected studies considered the following cultural characteristics: country and geographical location and organizational classification and size. These characteristics are presented based on the users' type as follows:

Residents: Country and Geographical Location. In Study #4, the results showed that all residential users (European, USA, and Indian) exhibited similar levels of both security hygiene and risky behavior regardless of their geographical location. The authors in study #13 showed that Africa and South Asia

Open Science Index, Computer and Information Engineering Vol:15, No:9, 2021 publications.waset.org/10012256.pdf

had the highest malware infection rates whereas North America and Europe had the lowest.

Employees: Country and Geographical Location. In study #10, the results showed that employees based in the US, Brazil, and India were at significantly reduced risk of being targeted compared to employees in China, Europe, and Australia.

Organizational Classification and Size: The results in study #10 revealed that a specific industry sector and larger organizations and individuals (specifically directors and managers) belonging to them are statistically at elevated risk compared with others.

Serveries Users: Country and Geographical Location. In study #19, the authors found that the country, mainly concentrated in Europe and Africa, represents a considerable risk factor. In study #9, the results showed that different countries had a different ratio of malware attacks. For instance, Japan appeared to have the lowest per-user ratio of malicious hits, whereas Mediterranean countries (namely France, Spain, and Italy) that share similarly high values of several risk indicators.

Students and Employees: The study that considered students and employees did not investigate the cultural characteristics.

iii. Personality

Researchers have used personality to clarify the cognitive method, behaviors, and behavioral effects of an individual [6], [7]. Personality is considered a significant component of human factors because it remains relatively constant throughout the life of an individual. User's personality characteristics were investigated by 16 out of 19 collected studies. Each group of the studied personality characteristics was placed on an individual row as shown in Table VI. Overall, we found that out of the total number of the studied user's personality characteristics, 42 of them were not duplicated. We summarized the findings of the selected studies based on the users' type as follows:

Academia: Study #2 found that spending more time on online activities did not increase the odds of victimization; antivirus programs had no significant impact on preventing malware infection; individuals who engage in media piracy were at an increased risk of victimization; those whose peers viewed pornography in cyberspace were at significant risk of malware infection, and the behavior of oneself and one's peers increases the risk of infection. In study #7, the researchers found that no relationship between legitimate computer use and malware infection, and they also found the following to be risk factors that correlated with malware attacks: participating in pirating media, viewing, sending harassing messages, and using someone else's Internet without authorization. The authors in study #16 found that a high volume of network usage was identified as a risk factor. Besides, visiting many web pages and certain categories of web pages were found to be a contributing risk factor. The researchers also found an association between the main web browser used and the risk of malware attack. Moreover, downloading executable files from the Internet, and engaging in P2P activity were both found to increase the risk of malware-attack.

Study #12 found that actual malware warnings generated significantly more activation in brain areas governing language comprehension, visual attention, and inspection. The study also found no statistically significant relationship between impulsivity (the less impulsive the individuals the better) and task performance. However, the authors observed that impulsive individuals' behavior showed significantly less brain activation and connectivity in regions governing decision-making and problem solving. The study also pointed that this could be counter-productive to phishing detection and malware warnings task performance.

Residents: In study #1, the authors showed that the usage of peer-to-peer, web, streaming, and chat applications, and Windows operating system as potential risk factors for malware infection. In study #4, the authors found that security hygiene had little correlation with observed behavior, whereas risky behavior (contact malicious sites even of being warned) more than doubled the likelihood of becoming infected with malware. Results from study #11 found that no concrete evidence, based on response efficacy, self-efficacy, and response cost, that malware victims were grossly negligent about security. They also found that victims do not relate value (large sums of money in a bank account), visibility (downloading and spending time on social media), and accessibility (weaknesses in software that can be used by fraudsters to attack customers) to victimization.

The authors in study #13 found the quality of technology in terms of bandwidth and speed, was found to be negatively correlated with the reduced malware infections. Besides, the study also found that individual investment in security (in terms of antivirus products) appeared to have a strong negative correlation with malware infections, that is individuals who tend to underestimate cybersecurity-related risk may tend to unprotect their computer. The authors of study #18 found that the use of two-factor authentication, data backup habits, encryption of a hard drive, frequency of using torrent services, password protection for login, and previous experience with online scams correlate with the risk of ransomware infection. The study also suggested that the relationship between the identified predictive factors and ransomware infection will likely change over time.

Employees: Study #8 investigated the VPN activity and browsing behaviors including categories of websites visited, web usage features, and blocked and low-reputation domains. The results showed that users who brought their machines outside often but spent less time on VPN were more exposed to threats; four categories namely chat, file transfer, social networks, and non-categorized sites contributed significantly to the risk of encountering malware attacks; the number of distinct domains visited by the host was strongly correlated with the encountering malware attacks, and the most significant domains that were most correlated with malware infection were visits to new domains and number of noncategorized sites that requiring user agreement.

In study #17, the results showed that self-efficacy, response efficacy, and security responsibility were significant predictors of employees' intentions to scan USB sticks with anti-malware software. Besides, the authors also found that for employees' intentions to not click on links in suspicious emails, self-

Open Science Index, Computer and Information Engineering Vol:15, No:9, 2021 publications.waset.org/10012256.pdf

efficacy, security breach experience at work, and perceived susceptibility were significant predictors. Moreover, the results also showed that for intentions to install software updates when prompted, response efficacy, response costs, perceived susceptibility, responsibility, and psychological ownership of data were significant predictors of malware attacks.

Serveries Users: In study #9, the authors found that the number of times the user surface the web and the period of the day a user is more active were at risk of infection. In study #15, the results showed that the number of unique binaries on users' machines was linked to the number of attacks, and the number of unsigned binaries on the users' machines was at higher risk than those with a less than median percentage of unsigned binaries. Besides, the number of binaries downloaded by users whose fraction of downloaded binaries was over the median value experience far more attacks than those whose fraction of downloaded binaries was below the median. Moreover, travel by a host machine showed a clear increase in the number of attacks.

For the security posture, study #19 suggested that many users who are at risk of attack have yet to enable additional protection. In terms of prior risk exposure, the study found that personal data exposed by third party breaches faced far higher average odds of an attack. Moreover, when compared to users owning multiple types of devices, the results showed that users who own only a personal computer faced slightly lower odds of targeting whereas mobile-only users faced even lower risks of an attack. Finally, for email activities, the odds of being targeted increase with the level of engagement with Gmail.

Students and Employees: Study #6 results showed that web browsing presented a higher rate of infection, especially sites such as sports and Internet infrastructure while more suspected sites such as pornography and illegal content were less in infection rate.

C. RQ2: How Do Susceptibility Factors Vary Based on the Type of Malware?

The purpose of RQ2 is to identify the susceptibility factors that vary based on the type of malware. This is important because different malware types are known to use different tactics, (e.g., differences in emotional processing; differences in frequency and type of computer usage; and risk perceptions), to trick users into downloading a file or clicking on a link inside an email. Table VII shows the susceptibility factors and malware types. As can be seen, the studied malware types were adware, virus, cracks, hack, exploit, rogue malware, Infostealer, ransomware, bot, rootkit, Trojan horse, AdClicker, ProcKill, Keylog, dropper, FakeAV, downloader, and backdoor. Out of the selected 19 studies, only three studies (namely: study #3, #8, and #14) considered the susceptibility factors vary based on the type of malware.

TABLE VII
THE SUSCEPTIBILITY FACTORS AND MALWARE TYPE

Study #	Author	Year	Susceptibility Factors: Demographics (D), Personality (P), Culture (C)	Malware Type
1	Carlinet et al. [5]	2008	P	Viruses and worms
2	Bossler and Holt [6]	2009	D and P	Viruses, worms and Trojan horse
3	Ngo and Paternoste [7]	2011	D	Virus, spyware,
4	Maier et al. [8]	2011	P and C	Family: Zlob, Conficker, and Zeus
5	Lee [9]	2012	D	Trojan, and others
6	Lévesque et al. [10]	2013	D and P	Trojan, Adware, Virus, Worm, Others
7	Holt and Bossler [11]	2013	D and P	Trojan, Adware, Virus, Worm, Others
8	Yen et. al. [12]	2014	D and P	Exploit, Ransom, AdClicker, ProcKill, Keylog, Dropper, FakeAV, Downloader, BackDoor.
9	Canali et al. [13]	2014	P and C	All type of malware provided by the Malware Domain List
10	Thonnard et al. [14]	2015	D and C	Trojans and worms and occasionally a virus
11	Jansen and Leukfeldt [15]	2016	P	Not specified (any type of malware)
12	Neupane et al [16]	2016	P	Not specified (any type of malware)
13	Levesque et al. [17]	2016	D, P and C	Not specified (any type of malware)
14	Lévesque et al. [18]	2017	D	Adware, virus, cracks, hack, exploit, rogue malware, infostealer, ransomware, bot, and rootkit
15	Ovelgonne et. al. [19]	2017	D and P	Viruses, worms, bots, trojans, etc.
16	Levesque et al. [20]	2018	D and P	Trojan, Adware, Virus, Worm, Others
17	Blythe and Coventry [21]	2018	P	Not specified (any type of malware)
18	Simoiu et al. [22]	2019	P	Ransomware
19	Simoiu et. al. [23]	2020	D, P and C	Emotet family, botnet's

In study #3, the results showed that the effect of age was identified as a significant predictor for computer virus infection, while gender was not found significant. Besides, the study also showed that older respondents being less likely to get infected by a computer virus. In study #8, researchers found that malware types differ by geographic location. For instance, while RDN/Generic and generic downloader can be found in all countries, exploits were the most common malware type in India, Brazil, and S. Korea, and Droppers are mostly found in China (attributed to the abundance of custom, free software available online). Additionally, study #8 also found that malware types vary based on the host type. For example, the

Open Science Index, Computer and Information Engineering Vol:15, No:9, 2021 publications.waset.org/10012256.pdf

study found that exploits target vulnerabilities in JavaScript and Java, though a non-trivial fraction of hosts also encountered PDF exploits and those targeting the Windows Shell. In study #14, the results suggested that the effect of age is not constant across different types of malware. The authors found that older users were more susceptible to rogue malware and ransomware.

IV. Discussions and Limitations

A. Discussions

Trends for User's Susceptibility Factors to Malware Attacks Studies: We have noticed that a lack of studies in users' susceptibility factors to malware attacks. This might be because that studies involving human subjects require approval from all entities involved, including the ethics board and IT department, which can lengthen the process and hence discouraging for most researchers [7].

Besides, starting from 2017 to 2020, the analytical model (data driven approach) has been the most adopted and used theoretical framework. This could be attributed to the new advances in big data and machine learning analytical techniques. We have also noticed that students are the most sample used by serval studies. This could be due to the facility of recruitment, lower cost of administration, and assumed lower response bias [32]. However, generalizing from students' samples to the general public has been found problematic when personal and attitudinal variables are utilized, as students vary mostly randomly from the general public across countries and variables [33].

Susceptibility factors and malware types: We have noticed that only three studies considered the relationship between susceptibility factors and malware types. As different types of malware use different tactics, (e.g., differences in emotional processing; differences in frequency and type of computer usage; and risk perceptions) to trick users into downloading a file or clicking on a link inside an email, considering this is important. The data from four studies showed that malware infections vary based on age, geographic location, and host types. For instance, older respondents being less likely to get infected by a computer virus, but more susceptible to rogue malware and ransomware. Besides, exploits target vulnerabilities in JavaScript, Java, and Windows Shell.

B. Limitation

This SLR aims to include as many available sources as possible, however, it is difficult to review all the literature. Thus, we decided to search for journal and conference publications in three leading scientific databases as the quality of the articles in these databases can be ensured. It should be noted that there are several unpublished articles such as companies' websites, white papers, technical reports, and forums and blogs that could add some value to our SLR, however, we believe that the quality of these sources is in general more difficult to be verified, and this could affect the external validity of the selected studies. As our focus was on the user's susceptibility factors to malware attacks, there could be some studies that perhaps studied users' susceptibility to malware attacks while not calling it by name, for instance: email-based attacks, spear phishing attacks, technical and automated solutions to prevent malware attacks, or social engineering-based attacks. Nevertheless, the main focus of these studies was rather on identifying the social engineering attacks or attackers.

V. Conclusions and Future Work

In this study, the susceptibility factors associated with a user falling for malware attacks as well as the variation of those factors based on the type of malware have been investigated using a SLR. We have developed detailed assessment criteria reflecting our research questions. Our search strategy included an automatic search of three digital libraries and snowballing. The data was extracted based on the developed assessment criteria from the primary studies. Our results from the 19 selected studies have shown that some demographic factors including type and level of expertise, level of education, and employment status are associated with malware infection regardless of the users' type (e.g., residents, employees, academia, etc.). On the other hand, age and gender are not consistent among the same and different types of users. Besides, we have also found that culture and personality factors are consistently associated with malware infection in most of the selected studies and for all types of users. Moreover, our results have shown that malware infection varies based on age, geographic location, and host types.

As per the results discussed in Section 3 and Section 4, we identify the following possible directions for future work. First, generalizing the results and risk of susceptibility factors to malware attacks from one user type to another could be problematic, as different types of users may be exposed to different threats or be targeted based on their user domains' characteristics. Future research in this field should consider this when analyzing and comparing users' susceptibility factors to malware attacks [35], [36]. Second, our data have shown that the cultural factors and their relationship to malware attacks among the academic users (universities: students and faculties) have not been investigated [37]-[39]

Third, few studies considered the relationship between susceptibility factors and malware types. As different types of malware use different tactics to trick users into downloading a file or clicking on a link inside an email, considering this by future studies is important. Fourth, the lack of studies on users' susceptibility factors to malware attacks might be because studies involving human subjects require approval from all entities involved, including the ethics board and IT department, which can lengthen the process and hence discouraging for most researchers [7], [40], [41]. Exploring further steps to enhance the process should be highly considered as more malware attacks are utilizing the social engineering techniques, such as spear phishing or email-based attacks, to target human vulnerabilities.

References

[1] S. Rob, "134 Cybersecurity Statistics and Trends for 2021," *Varonis*, Jan. 13, 2020. https://www.varonis.com/blog/cybersecurity-statistics/

(accessed Jan. 30, 2021).

[2] R. Anderson, "Why cryptosystems fail," in *Proceedings of the 1st ACM Conference on Computer and Communications Security*, 1993, pp. 215–227.

[3] A. Whitten and J. D. Tygar, "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0.," in *USENIX Security Symposium*, 1999, vol. 348, pp. 169–184.

[4] S. Clark, T. Goodspeed, P. Metzger, Z. Wasserman, K. Xu, and M. Blaze, "Why (Special Agent) Johnny (Still) Can't Encrypt: A Security Analysis of the APCO Project 25 Two-Way Radio System.," in *USENIX Security Symposium*, 2011, vol. 2011, pp. 8–12.

[5] C. Simoiu, C. Gates, J. Bonneau, and S. Goel, "'I was told to buy a software or lose my computer. I ignored it': A study of ransomware," *In Fifteenth Symposium on Usable Privacy and Security (SOUPS)*, p. 21, 2019.

[6] J. Jeong, J. Mihelcic, G. Oliver, and C. Rudolph, "Towards an Improved Understanding of Human Factors in Cybersecurity," in *2019 IEEE 5th International Conference on Collaboration and Internet Computing (CIC)*, 2019, pp. 338–345.

[7] R. Montanez Rodriguez, E. Golob, and S. Xu, "Human Cognition through the Lens of Social Engineering Cyberattacks," *arXiv e-prints*, p. arXiv-2007, 2020.

[8] P. Brereton, B. A. Kitchenham, D. Budgen, M. Turner, and M. Khalil, "Lessons from applying the systematic literature review process within the software engineering domain," *Journal of systems and software*, vol. 80, no. 4, pp. 571–583, 2007.

[9] S. Das, A. Dingman, and L. J. Camp, "Why Johnny doesn't use two factor a two-phase usability study of the FIDO U2F security key," in *International Conference on Financial Cryptography and Data Security*, 2018, pp. 160–179.

[10] P. Doerfler *et al.*, "Evaluating login challenges as adefense against account takeover," in *The World Wide Web Conference*, 2019, pp. 372–382.

[11] C. Wohlin, "Guidelines for snowballing in systematic literature studies and a replication in software engineering," in *Proceedings of the 18th international conference on evaluation and assessment in software engineering*, 2014, pp. 1–10.

[12] W. R. King and G. Torkzadeh, "Information systems offshoring: Research status and issues," *MIS quarterly*, vol. 32, no. 2, pp. 205–225, 2008.

[13] Y. Carlinet, L. Mé, H. Debar, and Y. Gourhant, "Analysis of Computer Infection Risk Factors Based on Customer Network Usage," in *2008 Second International Conference on Emerging Security Information, Systems and Technologies*, Cap Esterel, France, Aug. 2008, pp. 317–325, doi: 10.1109/SECURWARE.2008.30.

[14] A. M. Bossler and T. J. Holt, "On-line Activities, Guardianship, and Malware Infection: An Examination of Routine Activities Theory," vol. 3, no. 1, p. 21, 2009.

[15] F. T. Ngo, "Cybercrime Victimization: An examination of Individual and Situational level factors," vol. 5, no. 1, p. 21, 2011.

[16] G. Maier, A. Feldmann, V. Paxson, R. Sommer, and M. Vallentin, "An Assessment of Overt Malicious Activity Manifest in Residential Networks," in *Detection of Intrusions and Malware, and Vulnerability Assessment*, vol. 6739, T. Holz and H. Bos, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 144–163.

[17] M. Lee, "WHO'S NEXT? IDENTIFYING RISK FACTORS FOR SUBJECTS OF TARGETED ATTACKS," *In Proc. Virus Bull. Conf*, pp. 301–306, 2012.

[18] F. Lalonde Levesque, J. Nsiempba, J. M. Fernandez, S. Chiasson, and A. Somayaji, "A clinical study of risk factors related to malware infections," in *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, New York, NY, USA, Nov. 2013, pp. 97–108, doi: 10.1145/2508859.2516747.

[19] T. J. Holt and A. M. Bossler, "Examining the Relationship Between Routine Activities and Malware Infection Indicators," *Journal of Contemporary Criminal Justice*, vol. 29, no. 4, pp. 420–436, Nov. 2013, doi: 10.1177/1043986213507401.

[20] T.-F. Yen, V. Heorhiadi, A. Oprea, M. K. Reiter, and A. Juels, "An Epidemiological Study of Malware Encounters in a Large Enterprise," in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security - CCS '14*, Scottsdale, Arizona, USA, 2014, pp. 1117–1130, doi: 10.1145/2660267.2660330.

[21] D. Canali, L. Bilge, and D. Balzarotti, "On the effectiveness of risk prediction based on users browsing behavior," in *Proceedings of the 9th ACM symposium on Information, computer and communications security - ASIA CCS '14*, Kyoto, Japan, 2014, pp. 171–182, doi: 10.1145/2590296.2590347.

[22] O. Thonnard, L. Bilge, A. Kashyap, and M. Lee, "Are You at Risk? Profiling Organizations and Individuals Subject to Targeted Attacks," in *Financial Cryptography and Data Security*, vol. 8975, R. Böhme and T. Okamoto, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2015, pp. 13–31.

[23] J. Jansen and R. Leukfeldt, "Phishing And Malware Attacks On Online Banking Customers In The Netherlands: A Qualitative Analysis Of Factors Leading To Victimization," Jul. 2016, doi: 10.5281/ZENODO.58523.

[24] A. Neupane, N. Saxena, J. O. Maximo, and R. Kana, "Neural Markers of Cybersecurity: An fMRI Study of Phishing and Malware Warnings," *IEEE Trans.Inform.Forensic Secur.*, vol. 11, no. 9, pp. 1970–1983, Sep. 2016, doi: 10.1109/TIFS.2016.2566265.

[25] F. L. Levesque, J. M. Fernandez, and A. Somayaji, "National-level risk assessment: A multi-country study of malware infections," *In Proc. of WEIS*, pp. 1–30, 2016.

[26] F. L. Lévesque, J. M. M. Fernandez, and D. Batchelder, "Age and gender as independent risk factors for malware victimisation," presented at the Electronic Visualisation and the Arts (EVA 2017), Jul. 2017, doi: 10.14236/ewic/HCI2017.48.

[27] M. Ovelgönne, T. Dumitraş, B. A. Prakash, V. S. Subrahmanian, and B. Wang, "Understanding the Relationship between Human Behavior and Susceptibility to Cyber Attacks: A Data-Driven Approach," *ACM Trans. Intell. Syst. Technol.*, vol. 8, no. 4, p. 51:1-51:25, Mar. 2017, doi: 10.1145/2890509.

[28] F. L. Lévesque, S. Chiasson, A. Somayaji, and J. M. Fernandez, "Technological and Human Factors of Malware Attacks: A Computer Security Clinical Trial Approach," *ACM Trans. Priv. Secur.*, vol. 21, no. 4, p. 18:1-18:30, Jul. 2018, doi: 10.1145/3210311.

[29] J. M. Blythe and L. Coventry, "Costly but effective: Comparing the factors that influence employee anti-malware behaviours," *Computers in Human Behavior*, vol. 87, pp. 87–97, Oct. 2018, doi: 10.1016/j.chb.2018.05.023.

[30] C. Simoiu, A. Zand, K. Thomas, and E. Bursztein, "Who is targeted by email-based phishing and malware?: Measuring factors that differentiate risk," in *Proceedings of the ACM Internet Measurement Conference*, Virtual Event USA, Oct. 2020, pp. 567–576, doi: 10.1145/3419394.3423617.

[31] S. Lewallen and P. Courtright, "Epidemiology in practice: case-control studies," *Community Eye Health*, vol. 11, no. 28, p. 57, 1998.

[32] J. J. Arnett, "The neglected 95%: why American psychology needs to become less American.," 2016.

[33] P. H. Hanel and K. C. Vione, "Do student samples provide an accurate estimate of the general public?," *PloS one*, vol. 11, no. 12, p. e0168354, 2016.

[34] R. L. Baskerville and M. D. Myers, "Design ethnography in information systems," *Information Systems Journal*, vol. 25, no. 1, pp. 23–46, 2015.

[35] Xu, Shouhuai. "The cybersecurity dynamics way of thinking and landscape." In Proceedings of the 7th ACM Workshop on Moving Target Defense, pp. 69-80. 2020.

[36] Fang, Z., Xu, M., Xu, S. and Hu, T., 2021. A framework for predicting data breach risk: Leveraging dependence to cope with sparsity. IEEE Transactions on Information Forensics and Security, 16, pp.2186-2201

[37] Henshel, Diane, Char Sample, Mariana Cains, and Blaine Hoffman. "Integrating cultural factors into human factors framework and ontology for cyber attackers." In Advances in human factors in cybersecurity, pp. 123-137. Springer, Cham, 2016.

[38] Ferro, Lauren S., Andrea Marrella, and Tiziana Catarci. "A Human Factor Approach to Threat Modeling." In International Conference on Human-Computer Interaction, pp. 139-157. Springer, Cham, 2021.

[39] Ferro, Lauren S., and Francesco Sapio. "Another Week at the Office (AWATO)–An Interactive Serious Game for Threat Modeling Human Factors." In International Conference on Human-Computer Interaction, pp. 123-142. Springer, Cham, 2020.

[40] Jagatic, Tom N., Nathaniel A. Johnson, Markus Jakobsson, and Filippo Menczer. "Social phishing." Communications of the ACM 50, no. 10 (2007): 94-100.

[41] Hijji, Mohammad, and Gulzar Alam. "A Multivocal Literature Review on Growing Social Engineering Based Cyber-Attacks/Threats During the COVID-19 Pandemic: Challenges and Prospective Solutions." IEEE Access 9 (2021): 7152-7169

Open Science Index, Computer and Information Engineering Vol:15, No:9, 2021 publications.waset.org/10012256.pdf