electronics

MDPI

Review

Cyberstalking Victimization Model Using Criminological Theory: A Systematic Literature Review, Taxonomies, Applications, Tools, and Validations

Waheeb Abu-Ulbeh [1], Maryam Altalhi [2], Laith Abualigah [1,3,*], Abdulwahab Ali Almazroi [4], Putra Sumari [3] and Amir H. Gandomi [5,*]

1 Faculty of Computer Sciences and Informatics, Amman Arab University, Amman 11953, Jordan; w.abuulbeh@aau.edu.jo
2 Department of Management Information System, College of Business Administration, Taif University, Taif 21944, Saudi Arabia; marem.m@tu.edu.sa
3 School of Computer Sciences, Universiti Sains Malaysia, Pulau Pinang 11800, Malaysia; putras@usm.my
4 Department of Information Technology, College of Computing and Information Technology at Khulais, University of Jeddah, Jeddah 23218, Saudi Arabia; aalmazroi@uj.edu.sa
5 Faculty of Engineering and Information Technology, University of Technology Sydney, Ultimo, NSW 2007, Australia
* Correspondence: aligah.2020@gmail.com (L.A.); Gandomi@uts.edu.au (A.H.G.)

check for updates

Citation: Abu-Ulbeh, W.; Altalhi, M.; Abualigah, L.; Almazroi, A.A.; Sumari, P.; Gandomi, A.H. Cyberstalking Victimization Model Using Criminological Theory: A Systematic Literature Review, Taxonomies, Applications, Tools, and Validations. *Electronics* **2021**, *10*, 1670. https://doi.org/10.3390/electronics10141670

Academic Editor: Guillermo L. Taboada

Received: 9 June 2021
Accepted: 5 July 2021
Published: 13 July 2021

Abstract: Cyberstalking is a growing anti-social problem being transformed on a large scale and in various forms. Cyberstalking detection has become increasingly popular in recent years and has technically been investigated by many researchers. However, cyberstalking victimization, an essential part of cyberstalking, has empirically received less attention from the paper community. This paper attempts to address this gap and develop a model to understand and estimate the prevalence of cyberstalking victimization. The model of this paper is produced using routine activities and lifestyle exposure theories and includes eight hypotheses. The data of this paper is collected from the 757 respondents in Jordanian universities. This review paper utilizes a quantitative approach and uses structural equation modeling for data analysis. The results revealed a modest prevalence range is more dependent on the cyberstalking type. The results also indicated that proximity to motivated offenders, suitable targets, and digital guardians significantly influences cyberstalking victimization. The outcome from moderation hypothesis testing demonstrated that age and residence have a significant effect on cyberstalking victimization. The proposed model is an essential element for assessing cyberstalking victimization among societies, which provides a valuable understanding of the prevalence of cyberstalking victimization. This can assist the researchers and practitioners for future research in the context of cyberstalking victimization.

Keywords: cyberstalking victimization; criminological theory; routine activities; lifestyle exposure

1. Introduction

The Internet has been an integral part of daily life in recent years. The Internet user stats for 2020 show that more than 5 billion Internet users are distributed worldwide [1]; this indicates that the Internet is used by half of the world's people. The exponential spread of the Internet and other information and communication technology affect every area of life. The Internet has numerous features that make it attractive and explain its rapid penetration, such as ease of use, immediacy, law restrictions, low cost, and widespread availability [2]. On the other hand, there is a dark side to this increased Internet usage. The anonymous nature (the physical distance from others is irrelevant) of the Internet and using communication technologies gives perpetrators a vast opportunity to commit crimes, so the Internet has become a vital tool for facilitating the creation of the new phenomenon of "cybercrime" [3–14].

Cyberstalking is a cybercrime categorized as a crime and used as computer networks or devices to advance other ends [15]. While there is no widely accepted concept of cyberstalking, there are several guidelines to follow [8,16–37]. The most generally accepted definition is that the activities are carried out over the Internet or mobile devices [24]. Some researchers have argued that there is no agreed definition of cyberstalking (virtual) because there is no agreed-upon meaning (physical) [24,38]. The word "cyberstalking" is used interchangeably with "cyberharassment", "online stalking", or "online harassment" [24,30,39,40]. The dissemination of threats and false claims, data destruction, computer surveillance, identity stealing, and sexual motives [41–43], the persistent pursuit of an attacker using electronic or Internet-capable computers [44], electronic sabotage such as transmitting viruses or spamming, buying products and services in the victims' names, and sending false messages are all examples of cyberstalking [42,43]. Cyberstalking is a real threat facing our societies today. We should confront this new phenomenon by examining new modalities and looking for solutions to the issue, and reducing its damage to its victims [45–47].

There is a scarcity of information on cyberstalking in the literature, and further research is required to solve this issue. This paper focuses on cyberstalking victimization. The aim is to investigate it by estimating its prevalence and examining the relationships between factors to propose a conceptual model of cyberstalking victimization to increase understanding of this new phenomenon.

2. Background of the Study and Problem Statements

Over the last two decades, the development of the Internet and the exponential growth of the World Wide Web (WWW) have profoundly altered life in contemporary societies [48,49]. Using cyberspace takes up a significant amount of time in many people's daily lives [50–52]. In conjunction with the rapid development of ICTs, the Internet has created a near-perfect arena for crimes to occur [48]. The British Prime Minister, David Cameron, in a 2013 speech to the National Society for the Prevention of Cruelty to Children (NSPCC), said, "The internet is not only where we buy, sell, and socialize; it's also where violations occur, and people can be harmed".

Recently, the Internet has enabled new forms of cybercrime to emerge. Cyberstalking [6] is classified as using ICTs to carry out practices such as finding, surveying, harassing, or exploiting victims to cause anxiety, panic, or alarm and is characterized by the repetitive aspects of the behavior [53]. Cyberstalking is a real threat. The various forms of cyberstalking include sending harassing text messages, taking photos or videos of victims without their consent, sending malicious malware or spyware to the victim's email, sending false information or statements to others by using the victim's email directly, and monitoring the victim's email or computer [54].

In academic circles, cyberstalking is a relatively recent subject. However, it is also gaining traction as a research subject. It is possible to find studies on cybercrimes in general; however, few have tried systematically to propose a cybercrime model, specifically cyberstalking victimization, and empirically test it. Cyberstalking research is still in its infancy, and much more research is needed [25,31,55–58]. This gap is more noticeable in cyberstalking as a form of cybercrime than in other states. The lack of understanding of this new phenomenon comes from the lack of scientific definition [21]. A lack of statistics also plays a role in this misunderstanding [24,59]. Gnasigamoney and Sidhu [60], who conducted their study in Malaysia, found no statistics about cyberstalking in Malaysia. A prevalence measure is also needed [24,61] and research on the nature of cyberstalking [62].

Cyberstalking studies are neglected compared to physical stalking in the literature (28% and 59%, respectively) [63]. Little is known about cyberstalking [64], and data are limited due to the limited research on this topic [16]. Primary research is needed in terms of empirical work in various aspects of cybercrime and cyberstalking [8,29,37,65–71]. Although cyberstalking is a severe and growing problem and is recognized by researchers, it remains insufficiently examined [43,72]. To fill this gap in the literature, the present

research theoretically develops and empirically tests a proposed conceptual model for cyberstalking victimization in the Hashemite Kingdom of Jordan (hereafter Jordan). This model can help the executive, legislative and judicial authorities, citizens, lawmakers, and others to assess this phenomenon properly.

Cybercrime in Jordan is affecting society like other societies in the world. Jordan is one of only two Middle Eastern countries that has completely liberalized the telecommunications market. It has become the most advanced country in that region in terms of ICTs [73]. As a result of the spread of ICTs and the Internet, Internet users have jumped from 127,300 (in 2000) to 5,700,000 users (2020). Table 1 depicts Jordan's Internet users and population from 2000 to 2020, according to the world stats 2020. The Jordanian population was 10,909,567, and 80% were Internet users, giving 8,700,000 users, with 6,258,000 having a Facebook account.

Table 1. Internet usage statistics (2000–2020).

Year	Users	Population	% Pop.
2000	127,300	5,282,558	2.4
2002	457,000	5,282,558	8.7
2005	600,000	5,282,558	11.4
2007	796,900	5,375,307	14.8
2008	1,126,700	6,198,677	18.2
2009	1,595,200	6,269,285	25.4
2010	1,741,900	6,407,085	27.2
2012	2,481,940	6,508,887	38.1
2020	8,700,000	10,909,567	79.7

As shown in Table 1, the increase in the number of Internet users is significant compared to the growth in the population [74]. Therefore, it was not surprising that there is a real rise in the number of cybercrimes in Jordan. Cybercrimes pose a critical problem for the police force and judicial police in Jordan because of the unique technical nature of this crime [75].

With the lack of attention to cyberstalking in the Jordanian ISC Act, cyberstalking experiences have increased. In December 2015, the Criminal Investigation Department (CID) in Jordan created a Facebook page with the slogan "Towards Safe Cyberspace" to clarify the procedure for making a cybercrime complaint. However, the problem is still more extensive than the solution, and consequently, this research investigates cyberstalking victimization by estimating its prevalence and examining the relationships between factors. The results contribute to knowledge about this issue and help the government authorities assess cyberstalking victimization and increase citizens' awareness about this threat. The main question in this study is: "How can cyberstalking victimization be investigated?" Four subquestions focus on this research to answer the central question:

1. What is the prevalence of cyberstalking victimization among college students?
2. What are the relationships between L-RAT constructs and cyberstalking victimization?
3. What are the demographic factors that are linked to being a survivor of cyberstalking?
4. How do we develop a cyberstalking victimization model?

The objectives of this research are as follows:

1. To estimate the prevalence of cyberstalking victimization among college students.
2. To examine the relationships between L-RAT constructs and cyberstalking victimization.
3. To identify the demographic factors that are linked to the history of cyberstalking victimization.
4. To develop and validate a cyberstalking victimization model.

This paper focuses on students in Jordan. It is well-known that students frequently use the Internet, which exposes them to the risk of becoming a victim of cyberstalking victimization, making them attractive as a sample for this research. In terms of individuals, this research focuses on students registered at Luminus Technical University College (LTUC)

to investigate cyberstalking victimization. Including other students from other colleges in the sample would increase the time required for data collection without adding to the quality of the findings. Concerning criminal activities, this study focuses on cybercrime victimization, and specifically, cyberstalking. A group-administered questionnaire was used to collect data and was then evaluated in the SEM system using the partial least squares (PLS) technique. Microsoft Visio and Excel 2010, SmartPLS 2.0, and IBM SPSS 20 were used as analysis tools to develop the conceptual research model. In addition, QSR's NVivo 10 was used for the systematic literature review conducted in the current research. Lastly, Mendeley software was used as a management tool for references.

The significance of this paper is based on three main perspectives, which are as follows. First, this is the first survey study in Jordan to improve cyberstalking victimization at an educational, organizational level. To assess the current status of cyberstalking in Jordan, the results will advocate that the recommendations on dealing with such threats will force establishing a Jordanian Computer Emergency Response Team (JoCERT) in the countries. Second, and drawing from literature in the study field, there have been a few attempts to understand cyberstalking victimization worldwide, but unfortunately, none of them in Jordan. There is a lack of cyberstalking statistics and materials available to researchers and citizens. This study will be seen as comprehensive material for future research on this topic and contribute to knowledge.

Furthermore, the report supports the lifestyle routine activities theory (L-RAT) applicability for assessing simulated and physical crime victimization. Third, there are no studies that adequately develop theoretically and empirically test a model for cybercrime victimization and very few on cyberstalking victimization, so the theoretical findings and methodology employed in this study may be helpful in the fields of information systems (IS), criminology (cyber-criminology), psychology and sociology. Jordan is one of only two Middle Eastern countries to liberalize its telecommunications market. The growing use of the Internet and other technology has presented Jordanian society with problems, necessitating creating a legislative model to mitigate the negative consequences of Internet use. This research can be seen to fill in this gap to increase the understanding of this new aggressive phenomenon by examining the critical relationships between factors to prevent people from falling victim to cyberstalking victimization.

3. Theoretical Background

There is a lack of cyberstalking victimization studies in general which are mainly: a lack of studies showing the frequency of cyberstalking incidents, a lack of knowledge of the existence of cyberstalking and the consequences for victims [18,76], a lack of empirical research [70,71,77–79], a lack of documentation on the extent of cyberstalking [16,25,44,80,81], a lack of cyberstalking victimization studies on college students [76,82,83], a lack of victim statistics for those who are cyberstalked or harassed, a lack of range and a lack of appropriate tracking methods [78,84], a lack of knowledge about cyberstalking [77,85–87], as well as a misunderstanding of what causes cyberstalking [81,88] and a lack of theories for assessing the factors of guardianship in cyberstalking [88].

To explain the definition of violence, researchers have used a variety of methods. Routine behaviors and lifestyle exposure hypotheses are the most commonly used theories. Both theories are called incentive theories because they relate criminality to illegal opportunities present in everyday life. Routine behaviors and lifestyle risk hypotheses ignore violent proclivity and instead rely on the circumstances in which crime occurs. It is difficult to differentiate between the two, according to Yucedal [37], since both hypotheses share similar assumptions. Both hypotheses rely on how individuals' lifestyles or everyday routine behaviors provide opportunities for criminals to commit crimes. According to Miethe and Meier [89], the distinction between the two is in the language and focus used to describe crime and victimization risk. Cohen and Felson [90] suggested the routine practices hypothesis, which offers a systematic justification for criminal victimization, including logically, by integrating the three factors in time and space: driven criminals,

fitting aim, and absence of guardianship. On the other hand, Hindelang, Gottfredson, and Garofalo [91] introduced the lifestyle exposure hypothesis to understand generational variations in the probability of personal victimization.

Routine Activities Theory. Lawrence E. Cohen and Marcus Felson introduced the repetitive tasks principle in 1979 [90]. It describes crime by combining three factors: driven criminals, a desirable target, and the lack of competent guardianship. Crime happens as these elements collide in time and space. The absence of all of these factors, according to Yucedal [37], avoids the incidence of criminal and deviant conduct. The hypothesis was created to understand why crime rates in the United States increased after World War II. According to a 1979 study by Cohen and Felson [90], the increased rate of crime in the 1960s and 1970s was due to changes in social life, which increased criminal opportunities after WWII, especially as women began to join the workforce, resulting in a decrease in the number of household members, leading to more time spent away from home, creating more opportunities for offenders. In addition, changes in social life limited the number of family guardianship members and forced them into closer interaction with suspected criminals. Their increased exposure and mobility provided more chances for motivated offenders to identify viable unprotected targets.

Lifestyle Exposure Theory. According to Hindelang et al. [91], who analyzed data from eight American cities, the probability of victimization is determined by an individual's lifestyle, which is characterized as repetitive everyday activities, such as work and school as vocational activities, and leisure activities, such as play and socializes. The study also discovered that different behaviors expose people to various circumstances and that these lifestyles put people at a higher risk of being victimized due to their exposure. Furthermore, the researchers claim that people who spend more time in public places, especially at night and with non-family members, are more likely to be victims of personal crimes. Being in public places is directly related to people's lifestyles. The study also claims that different demographic and socio-economic characteristics, such as family income, sex, marital status, and age, are linked to being victims of personal crimes.

Lifestyle Routine Activities Theory (L-RAT). Lifestyle routine activities theory (L-RAT) [48] combines the concepts of routine activities theory with the lifestyle exposure theory proposed by Hindelang [91] and colleagues. According to Cohen et al. [92], the lifestyle explanation holds that victimization is the product of repetitive habits and behaviors that increase exposure to empowered criminals and decrease exposure to competent guardians. Furthermore, according to Reyns [64], two ideas have been indirectly mixed over the years, and scholars have tested hypotheses on how the environment and repetitive behaviors subject people to the risk of victimization. In a 2014 publication, Sissing stated that the two hypotheses collide at the concept of the lifestyle exposure hypothesis, which states that people exercise their various habits by following their own everyday routine behaviors. This means that demographic characteristics such as age, gender, and ethnicity influence people's lifestyles and victimization rates.

Furthermore, Cohen et al. [92] found that the lifestyle concepts of occupational and recreational tasks are integrated with the regular activities definition of a desirable goal in another analysis. An individual's lifestyle, everyday habits, and behaviors, according to L-RAT, are what make them appropriate targets [93]. Meanwhile, Choi [94] claims that the two hypotheses are not mutually exclusive; instead, the repetitive behaviors hypothesis extends the lifestyle exposure theory. Victimization rises as a result of "lifestyle changes", according to Miethe et al. [95], and repetitive habits and lifestyle exposure hypotheses include two fundamental conclusions regarding the existence and determinants of criminal victimizations. The first is that criminality happens as motivated criminals, convenient targets, and no third-party guardian come together in time and place. The second theory is that such repetitive habits and/or behaviors (frequent night-time or daytime movement outside the home) are riskier than others because they expose a target to more prospective criminals, increase exposure, and/or reduce guardianship. The hypotheses of the two theories were combined into two core propositions by Miethe and Meier [89]: first, routine

behavior habits and lifestyles increase the interaction between future criminals and suspects, resulting in a criminal incentive structure; second, the intrinsic importance of an objective and its guardianship value decide the preference of specific crime victims. They also noted that in the theoretical model of victimization known as the "structural-choice" model, proximity and accessibility to motivated criminals are considered "structural" elements.

In contrast, goal appearance and guardianship are considered "choice" components. Thus, exposure and proximity are viewed as systemic characteristics because their patterns of social interactions predispose people to high-risk settings and circumstances. At the same time, appearance and guardianship are thought to decide the preference or selection of specific goals for victimization.

Lifestyle Routine Activities Key Factors. Cohen, Kluegel, and Land [92] were the first to specifically present the L-RAT by defining the causes and relationships between demographic features and victimization, including exposure, proximity, attractiveness, guardianship, and crime definitional properties. The integrated theory L-RAT is similar in its key concepts to the original theories (RAT and lifestyle exposure), such as suitable target vs. target attractiveness, proximity to motivated offenders, and motivated offenders. Vakhitova et al. [96] stated that the main concepts are not evident in the models that were introduced, and it did depend on how the researchers defined. The key factors in the literature will be depicted in the following section, followed by the empirical test supporting the physical world, then the virtual world overview. The location or exposure of motivated criminals reveals the offender's involvement in a criminal case. Exposure is characterized as "the physical presence and accessibility of individuals and items to potential offenders at any given time or location" [92]. Proximity is defined as "the physical gap between places where potential targets of crime live and areas where comparatively significant populations of potential offenders are present." The two meanings happen to have a lot in common. According to Felson [97], a driven criminal is "anyone with a desire to commit the crime", while Bratt [98] defined it as "a person who is motivated to commit the crime." The question now is: what makes a motivated offender? It is an amalgamation of various factors, including gain vs. need, society, experience, the environment, and the associated beliefs. Scholars have identified proximity as a neighborhood characteristic, and since motivated criminals live locally, high-crime locations are more likely to be attacked [99]. In addition, social-economic features of the place of residence were used to operationalize proximity to motivated criminals, such as average wage, unemployment rate, the form of living (urban vs. rural), and others [96]. In the literature, exposure has also been operationalized using variables representing different degrees and types of activities. These metrics include the number of nights a week spent engaged in recreational activity outside the residence, the number of hours per week the house is unoccupied, etc. According to Cohen et al. [92], the greater the likelihood of criminal victimization, the closer possible targets live to comparatively large populations of motivated criminals. As a result, increasing visibility raises the risk of becoming a survivor.

Finkelhor and Asdigian [100] suggested the expressions of gratifiability, antagonism, and insecurity to assess goal attractiveness. The inspired criminal perceives a gratifying goal as rewarding. On the other hand, an antagonistic target can elicit a harsh response from a motivated offender. A weak target is seen as unable or unable to overcome a motivated offender. Felson and Clarke [101] developed a list of characteristics that raise the likelihood of victimization: value, inertia, exposure, and access (VIVA). Worth refers to the target's monetary value, inertness to its weight, visibility to its appearance, and accessibility to its functionality [96] (see Figure 1).

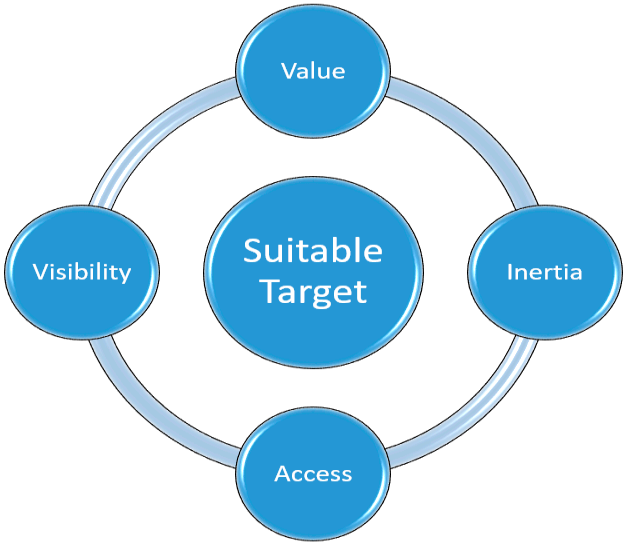

Figure 1. Suitable target–VIVA model.

According to Burke [102], an appropriate subject is an individual or item of interest or things or people on whom criminality is aimed, such as an object to rob or a person to strike [98]. Clarke and Webb [103] presented the "CRAVED" model of stealing objectives, which identified six essential properties for goods: concealable, removable, accessible, valuable, pleasant, and disposable [104]. They define "concealable" as items concealed in pockets or bags, making them more vulnerable to shoplifters and other stealth thieves. The fact that automobiles and motorcycles are mobile, i.e., disposable, explains why they are often stolen. The term "open" refers to the concept that "desirable items that are easily available and easy to find are more vulnerable." Visibility and usability are classified as "availability" in the VIVA model. Thieves will usually prefer the more costly or "valuable" items, particularly if they want to sell them. The notion that residential burglars are more likely to steal videos and televisions than similarly available or expensive electronic products such as microwave ovens or food processors is also defined as "enjoyable" by Clarke and Webb [103], which represents the pleasure-loving lifestyle of many criminals and the people who buy from them. The last property is "disposable", which refers to thieves like items that are simple to sell (see Figure 2).

Figure 2. Suitable target–CRAVED model.

Capable Guardianship. Cohen et al. [92] characterize guardianship as the ability of individuals such as housewives, neighbors, private security guards, and pedestrian law enforcement officers, as well as items such as locks, burglar alarms, and blocked windows, to deter crimes from happening, either through their presence alone or through some form of direct or indirect intervention. This definition reflects the assumption for guardianship, i.e., the greater the guardianship, the less the risk of criminal victimization. The purpose of guardianship has evolved, and scholars now typically operationalize it to include social guardianship (focusing on presence and action). Miethe and Meier [105] conceptualized capable guardianship as having both personal (and social) and physical measurements. The individual (social) component is intriguing since a human aspect, such as neighbors, police or friends, has a crime-prevention impact. In contrast, the physical dimension reflects the use of target-hardening techniques such as burglar alarms, locks, self-preservation skills and others. Cohen and Felson [90] refer to capable guardianship as "ordinary citizens", while Burke [102] describes it as "people or objects that deter crime" (see Figure 3).

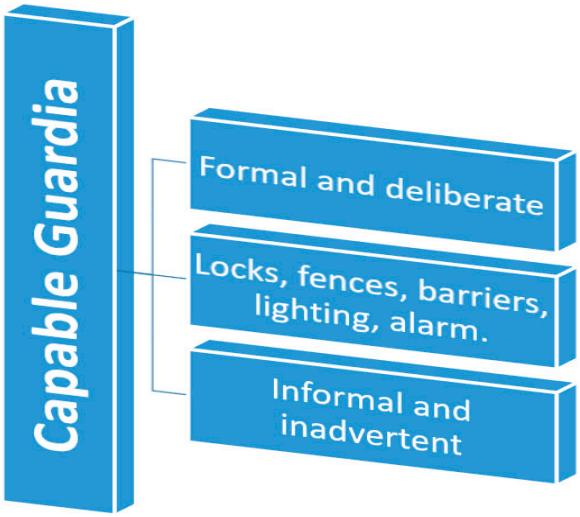

Figure 3. Capable guardianship model.

Empirical Testing of L-RAT on Physical World. The hypothesis of lifestyle routine activities (L-RAT), which has been used widely to describe various forms of physical victimization, is generally supported by the body of study in the literature. The lifestyle routine behaviors viewpoint has been used to describe multiple forms of victimization, such as theft, rape, abuse, arson, assault, larceny, and robbery, as seen in Table 2. However, this scientific viewpoint has not been thoroughly investigated as an explanation for harassment, with only three experiments specifically using the lifestyle repetitive behaviors method to explain stalking victimization [88,106,107]. In summary, the lifestyle routine tasks viewpoint has been seen to help understand victimization in the real world, but further research is required to know if it is still valuable for explaining victimization in the virtual world.

Table 2. Empirical testing of L-RAT on physical world.

No.	Reference	Sample	Dependent Variable
1	Cohen and Cantor (1981) [108]	National Crime Survey (NCS)	Burglary victimization
2	Jensen and Brownfield (1986) [109]	Monitoring the Future (MTF)	Property, violence, and vandalism victimization
3	Miethe et al. (1987) [110]	National Crime Survey (NCS)	Property and violent victimization
4	Sampson (1987) [111]	British Crime Survey (BCS)	Personal violence and theft
5	Sampson and Wooldredge (1987) [112]	British Crime Survey (BCS)	Larceny victimization, personal and household theft, and burglary
6	Lasely (1989) [113]	British Crime Survey (BCS)	Predatory victimization
7	Kennedy and Forde (1990) [114]	Canadian urban victimization survey	Vehicle theft, breaking and entering (B&E), assault, and robbery victimization
8	Miethe and Meier (1990) [89]	British Crime Survey (BCS)	Burglary, theft, and violent victimization
9	Sampson and Lauritsen (1990) [115]	British Crime Survey (BCS)	Assault victimization, stranger assault, acquaintance assault
10	Lauritsen et al. (1991) [116]	National Youth Survey (NYS)	Assault, robbery, larceny and vandalism
11	Lauritsen et al. (1992) [117]	National Youth Survey (NYS); Monitoring the future (MTF)	MTF: Assault; NYS: Assault and robbery victimization
12	Wooldredge et al. (1992) [118]	Survey University faculty members	Personal and property victimization
13	Miethe and McDowall (1993) [119]	Survey of adults in Seattle	Burglary victimization and violence by strangers
14	Rountree et al. (1994) [120]	Survey of adults in Seattle	Burglary and violent victimization
15	Schwartz and Pitts (1995) [121]	Undergraduate students from Ohio University	Rape
16	Fisher et al. (1998) [122]	Nationally representative sample in the U.S.	On-campus theft victimization and violent
17	Mustaine and Tewksbury (1998) [123]	Survey of college students	Major and minor theft victimization
18	Mustaine and Tewksbury (1999) [124]	University women in 9 institutions	Stalking
19	Fisher et al. (2000) [106]	College women in U.S.	Sexual victimization
20	Mustaine and Tewksbury (2000) [125]	Survey of college students	Assault victimization
21	Wittebrood and Nieuwbeerta (2000) [126]	Survey of adults in the Netherlands	Personal larceny, threat, sexual assault, burglary, car and bicycle theft victimization
22	Fisher et al. (2001) [127]	National representative sample in the U.S.	Stalking
23	Mustaine and Tewksbury (2002) [128]	Survey of college women	General and serious sexual assault victimization
24	Schreck et al. (2002) [129]	Survey of students in Fayetteville	Violent victimization
25	Dugan and Apel (2003) [130]	National Crime Victimization Survey (NCVS)	Violent victimization of women
26	Schreck et al. (2003) [131]	National Household and Education Survey, School Safety and Discipline (NHES-SSD)	Overall, property and violent victimization at school
27	Schreck and Fisher (2004) [132]	National Longitudinal Study of Adolescent Health (Add Health)	Violent victimization

Table 2. *Cont.*

No.	Reference	Sample	Dependent Variable
28	Tseloni et al. (2004) [133]	National Crime Victimization Survey (NCVS), British Crime Survey (BCS) and Police Monitor (PM)	Burglary victimization
29	Schreck et al. (2006) [134]	Gang Resistance Education and Training (GREAT) program	Victimization
30	Wilcox et al. (2007) [135]	Survey of adults in Seattle	Burglary victimization
31	Messner et al. (2007) [136]	Survey of adults in China	Personal theft, swindling, robbery, and assault victimization
32	Taylor et al. (2007) [137]	Survey of eighth-graders in public school	Violent and serious violent victimization
33	Taylor et al. (2008) [138]	Survey of eighth-graders in public school	Serious violent victimization
34	Spano et al. (2008) [139]	Mobile Youth Survey	Violent victimization
35	Burrow and Apel (2008) [140]	National Crime Victimization Survey (NCVS)—School Crime Supplement	Larceny and assault victimization at school and in the community
36	Wilcox et al. (2009) [141]	Rural Substance Abuse and Violence Project (RSVP)	Assault and theft victimization
37	Savolainen et al. (2009) [142]	Survey of adolescents in Helsinki	Violent victimization
38	Reid and Sullivan (2009) [143]	Developmental Victimization Survey	Bullying and general victimization
39	Henson et al. (2010) [144]	Survey of students from rural Kentucky high school	Minor and serious violent victimization
40	Fisher et al. (2010) [145]	National College Women Sexual Victimization study (NCWSV)	Sexual victimization and repeat sexual victimization
41	Tillyer et al. (2010) [146]	Rural Substance Abuse and Violence Project (RSVP)	Sexual harassment and assault victimization
42	Shubak Tillyer et al. (2011) [147]	National Longitudinal Study of Adolescent Health (Add Health)	Violent victimization
43	Tillyer et al. (2011) [148]	Rural Substance Abuse and Violence Project (RSVP)	Serious violent victimization
44	Peguero et al. (2015) [149]	Education Longitudinal Study (ELS)	Property and violent victimization at school
45	Pauwels and Svensson (2011) [150]	School surveys in Sweden and Belgium	General victimization
46	Averdijk (2011) [151]	National Crime Victimization Survey (NCVS)	Household and violent victimization
47	Peguero and Popp (2012) [152]	Education Longitudinal Study (ELS)	Violent victimization at school
48	Maimon and Browning (2012) [153]	Project on Human Development in Chicago Neighborhoods (PHDCN)	Violent victimization

Table 2. *Cont.*

No.	Reference	Sample	Dependent Variable
49	Bunch et al. (2015) [154]	National Crime Victimization Survey (NCVS)	Violent and theft victimization
50	Gibson et al. (2014) [155]	Project on Human Development in Chicago Neighborhoods (PHDCN)	Violent victimization (by neighborhood disadvantage)
51	Reyns et al. (2016) [88]	Canadian general social survey	Stalking victimization

Empirical Testing of L-RAT in Virtual World. Phillips [93] stated that despite having been applied to various crimes in the physical world, using the lifestyle routine activities theory in the virtual world is still limited. According to Back [77], the theoretical integration (L-RAT) is essential to help explain the new crime phenomenon. A sparse amount of literature has been found on L-RAT or RAT as part of the explanation of victimization in cybercrimes. As can be seen in Table 3, the lifestyle routine activities approach has been utilized to explain different types of cybercrime victimization. Yet this theoretical approach remains relatively untested in explaining cyberstalking or cyberharassment. Only a few studies have used the L-RAT or RAT as a subset to understand the factors that increase the risk of becoming a victim of this new type of cybercrime. Eleven studies on this type of cybercrime were found in the literature: Holt and Bossler [156], Bossler et al. [157], Reyns et al. [44], Welsh and Lavoie [158], Marcum [159], Ngo and Paternoster [160], Marcum et al. [161], Leukfeldt and Yar [162], Back [77], Phillips [93] and Yucedal [37].

Table 3. Empirical testing of L-RAT in the virtual world.

Reference	Sample	Dependent Variable(s)
Hutchings and Hayes (2009) [163]	104 residents of Brisbane metropolitan area	Phishing
Choi (2008) [94]	204 college students	Computer crimes
Pratt et al. (2010) [164]	992 adults in Florida	Consumer fraud
Van Wilsem (2011) [165]	4353 Dutch households	Threat
Leukfeldt (2014) [166]	8379 Dutch populations	Phishing
Van Wilsem (2013) [167]	6201 Dutch households	Consumer fraud
Bossler and Holt (2009) [65]	570 college students	Malware infection
Alshalan (2006) [168]	987 national cybercrime victimization survey (2004)	Cybercrime victimization
Holt and Bossler (2008) [156]	578 college students	Online harassment
Bossler et al. (2012) [157]	434 middle and high school students	Online harassment victimization
Navarro and Jasinski (2012) [169]	935 national sample of teenagers	Cyberbullying
Reyns et al. (2011) [82]	974 college students	Cyberstalking victimization
Welsh and Lavoie (2015) [158]	321 female undergraduate students	Cyberstalking victimization
Marcum (2008) [159]	483 freshmen college students	Online harassment, unwanted exposure to sexual materials, solicitation of sex online
Ngo and Paternoster (2011) [160]	295 undergraduate students	Cybercrime victimization (online harassment)
Marcum et al. (2010) [170]	744 undergraduate students	Unwanted sexually explicit material, unwanted sexual harassment, unwanted sexual solicitation

Table 3. *Cont.*

Reference	Sample	Dependent Variable(s)
Leukfeldt and Yar (2016) [162]	9161 Netherlands statistics	Hacking victimization, malware infection victimization, identity theft, consumer fraud victimization, cyberthreat victimization, cyberstalking victimization
Back (2016) [77]	1000 online South Korean users	Cyberharassment
Phillips (2015) [93]	274 college students	Cyberharassment, cyberstalking, cyber impersonation, sexting
Reyns (2013) [171]	5985 British Crime Survey (BCS)	Identity theft
Yucedal (2010) [37]	626 National Crime Victimization Survey (NCVS)	Computer virus victimization, online harassment victimization

4. The Proposed Cyberstalking Victimization Conceptual Model

A conceptual model is a well-specified model showing the fundamental relationships of a given set of variables as hypothesized from the theory [172]. Guba and Lincoln [173] adapted the view by Bamasoud [174], which found in his study that, if the following points are taken into consideration, i.e., the objective reality can be systematically and rationally investigated empirically and guided by the laws applied to social science; the independency of the researcher and the phenomenon being studied; the researcher remains detached; neutral objective; and propositions are generated by theories that are operationalized as hypotheses and have undergone experimental testing that is replicable, then the research is categorized as positivist.

The present research aimed to propose a conceptual model for cyberstalking victimization using the L-RAT perspective and empirically testing the hypotheses that were operationalized by the theories. As a result, the positivist paradigm is used to respond to the research questions in this study. The quantitative analysis methodology was selected to address the research questions because this study is concerned with testing hypothesis relationships and using the positivist model. In this research, a group-administered questionnaire was used to test the hypotheses. In this type of survey, a sample of respondents was requested at a familiar place and time, and each one was asked to fill the survey questionnaire at that place. According to Bhattacherjee [175], this format is convenient for the researcher and assures a high response rate. The scope of this study is to set students in Jordan, as it is well known that college students frequently use the Internet, with 90% of them accessing it daily [176], which exposes them to the risk of becoming a victim of cyberstalking victimization, through online social networking, texting, and instant messages [82]. Since college students have been identified as a high-risk demographic, they are a perfect community to research cyberstalking victimization [44]. Therefore, the target demographic for this study was college students, which corresponded to the study's theme of cyberstalking victimization.

The sample was selected from students from one college in Jordan for various reasons. Firstly, since cyberstalking victimization is not dependent on whether students are from colleges or schools, there was no reason to believe that students from different colleges would experience victimization differently. Any of them could become a victim of this new phenomenon. Secondly, including students from various colleges would increase the time required for data collection without any expected impact on the quality of the results. Thirdly, the college students' stakeholders asked the researcher to conduct the study in their college due to the importance of investigating the students' increasing experience of cyberstalking victimization. Fourthly, in exploring this new phenomenon or behavior, the most appropriate sampling type was to choose convenience sampling and focus on one student college and pay more attention to the process of data collection and concentrate on the finding's analysis. Fifthly, the student college that was selected had many distinguishing features that put it ahead of all other colleges in Jordan: it is the first and only college

in Jordan to have been internationally approved by the accreditation board for higher education programs in Britain Edexcel (BE); it has taught life skills in collaboration with the international organization for youth and Microsoft; it teaches English language materials intensively through the British Bell Center; it contains a business incubator; it is also connected with the largest and most modern fleet of transport for community colleges in Jordan, and it also has a section dedicated to consulting and recruiting students and graduates. Finally, it is geographically located in the middle of Jordan, specifically in the center of the capital Amman, making it an optimal environment to conduct this study. For these reasons, Luminus Technical University College (LTUC) was chosen as the college in the present research, and the respondents were the students. Inappropriateness, inadequacy, or excessive sizes of sample continue to influence the quality and accuracy of the study.

Questionnaire Design. The initial conceptual model for this study was drawn based on the systematic literature review because its relevant hypotheses were proposed. The next step is to design the questionnaire to collect the relevant information essential for this study. A questionnaire is a written set of questions to which respondents record their answers [177]. The questionnaire, which Sir Francis Galton invented, is defined as a researcher tool having a set of questions (items) planned to take responses from respondents in a consistent way [175]. Not only are the content and sequence of the questions necessary, but also how the questionnaire looks. The questionnaire should be laid out and presented very well. The current questionnaire started with a proper introduction that talked about cyberstalking (the main topic) and how this new phenomenon was distributed globally and locally and introduced the purpose of the study. The introduction also clearly disclosed the researcher's identity by giving his name and email address, contact hand phone (HP) numbers, and the university department to which he belongs. The length of the questionnaire was kept within reasonable limits [178]. In addition, the current questionnaire motivated the respondents through specific phrases such as "we strongly believe that your feedback is essential" and "it would be greatly appreciated if you could take the time to complete the questionnaire". The questionnaire ended on a courteous note with "Thank you for your time; your cooperation is highly appreciated." This note reminded the respondents to double-check that they had completed all the tasks.

The study's original model contained three independent variables: proximity to motivated criminals, appropriate aim (target attractiveness), and digital guardianship, as well as one single dependent variable: victimization due to cyberstalking. Proximity to motivated offenders is the first variable of L-RAT—the items were adapted from previous work on this area, with the things developed based on the activities that Jordanian society is interested in. After refining the measures, the items for this construct were operationalized using 23 items by asking the respondents: in the past, which of the following activities did you frequently do online? The answer choices were: hacking, political websites, e-banking, showing goods and services, job-seeking websites, e-government, health-care services, chatting/instant messenger (video), chatting/instant messenger (voice), chatting/instant messenger (text), social networking sites, sending/receiving emails, reading newspapers/magazines, playing games, watching TV programs, downloading computer programs, watching/downloading movies, listening to/downloading music, visiting religious websites, shopping, visiting adult websites, sport, adding unknown friend.

Formulating Measurement Model. The result of the instrument development was used to measure the proposed variables shaped as the conceptual model's constructs. In their study, Hair et al. [179] identified that the model that comprises the indicators and their associations with the constructs is called the "measurement model" or "outer model". According to Edwards and Bagozzi [180], measures can be referred to as "reflective indicators" when they are used to inspect an underlying construct that is unobservable (latent variable). In contrast, indicators that determine a construct are called "casual/formative indicators." MacCallum and Browne [181] mentioned that an unobservable construct that consists of reflective indicators is called a "reflective construct", while a construct comprised of causal indicators is called a "formative construct." The designation of a construct

as formative or reflective is somewhat illusive in many fields, including information systems. In the literature, many constructs that are used in IS are neither purely reflective nor purely formative. Previous research on IS showed that 30% of the constructs are misspecified [182]. Developing and analyzing a research questionnaire is directly related to the method of producing a measurement model. Therefore, when creating a research model, the researcher should consider two different measurement models: reflective and formative. Hair et al. [179] recommended guidelines for researchers to decide whether to measure a construct reflectively or formatively (see Table 4).

Table 4. Guidelines for choosing the measurement model method [117].

Criterion	Decision	Reference
The indicator's and the construct's causal priority	From the construct to the indicators: reflective. From the indicators to the construct: formative	Diamantopoulos and Winklhofer (2001) [183]
Is the build a trait or a mixture of indicators that explains the indicators?	• If trait: reflective. If combination: formative	Fornell and Bookstein (1982) [184]
Do the metrics reflect the construct's effects or causes?	• If consequences: reflective. If causes: formative	Rossiter (2002) [185]
Is it accurate that if the trait's evaluation changes, all things will change in the same way (assuming they're all similarly coded)?	• If yes: reflective. If no: formative	Chin (1998) [186]
Is it possible to swap out the items?	• If yes: reflective. If no: formative	Jarvis et al. (2003) [187]

In the current study, these guidelines were used to develop the questionnaire and select the appropriate assessment method. In the policies proposed by Hair et al. [179], four variables (proximity of motivated offenders, a suitable target, digital guardianship and cyberstalking victimization) were specified as reflective constructs (see Table 5).

Table 5. Measurement model decision.

Construct	Items	Criteria					Reflective/ Formative
		1	2	3	4	5	
Proximity to Motivated Offenders	Unknown Friend	√	√	√	√	√	Reflective
	Visiting Religious Websites	√	√	√	√	√	Reflective
	Listening/Downloading Music	√	√	√	√	√	Reflective
	Watching/Downloading Movies	√	√	√	√	√	Reflective
	Downloading Computer Programs	√	√	√	√	√	Reflective
	Watching TV Programs	√	√	√	√	√	Reflective
	Playing Games	√	√	√	√	√	Reflective
	Reading Newspapers/Magazines	√	√	√	√	√	Reflective
	Sending/Receiving Emails	√	√	√	√	√	Reflective
	Social Networking Sites	√	√	√	√	√	Reflective
	Chatting/Instant Messenger (Text)	√	√	√	√	√	Reflective
	Chatting/Instant Messenger (Voice)	√	√	√	√	√	Reflective
	Chatting/Instant Messenger (Video)	√	√	√	√	√	Reflective
	Health-Care Services	√	√	√	√	√	Reflective
	E-Government	√	√	√	√	√	Reflective
	Job-Seeking Websites	√	√	√	√	√	Reflective
	Showing Goods and Services	√	√	√	√	√	Reflective
	E-Banking	√	√	√	√	√	Reflective
	Political Websites	√	√	√	√	√	Reflective
	Hacking	√	√	√	√	√	Reflective
	Shopping	√	√	√	√	√	Reflective
	Visiting Adult Websites	√	√	√	√	√	Reflective
	Sport	√	√	√	√	√	Reflective

Table 5. *Cont.*

Construct	Items	Criteria					Reflective/ Formative
		1	2	3	4	5	
Suitable Target/Target Attractiveness	Name	√	√	√	√	√	Reflective
	Gender	√	√	√	√	√	Reflective
	Age	√	√	√	√	√	Reflective
	Mobile Phone Number	√	√	√	√	√	Reflective
	Email Address	√	√	√	√	√	Reflective
	Home Address	√	√	√	√	√	Reflective
	Bank Account Number	√	√	√	√	√	Reflective
	Study Program	√	√	√	√	√	Reflective
	Credit Card Serial	√	√	√	√	√	Reflective
	Favourite Activities	√	√	√	√	√	Reflective
	Photos	√	√	√	√	√	Reflective
	Videos	√	√	√	√	√	Reflective
Digital Guardianship	Antivirus Software	√	√	√	√	√	Reflective
	Antispyware Software	√	√	√	√	√	Reflective
	Firewall Software	√	√	√	√	√	Reflective
	Ad-Aware Software	√	√	√	√	√	Reflective
	Tracking Protection Blocks Software	√	√	√	√	√	Reflective
	Filtering/Monitoring Software	√	√	√	√	√	Reflective
	Changeyour Login Password	√	√	√	√	√	Reflective
	SaveExtra Copies	√	√	√	√	√	Reflective
	Create a Backup Process	√	√	√	√	√	Reflective
	Delete Old Files	√	√	√	√	√	Reflective
	Delete Old Emails/Attachments	√	√	√	√	√	Reflective
	Change any File Locations	√	√	√	√	√	Reflective
Cyberstalking victimization	Harassment	√	√	√	√	√	Reflective
	Defamation	√	√	√	√	√	Reflective
	Sexual Materials	√	√	√	√	√	Reflective
	Pretending to be you	√	√	√	√	√	Reflective
	Disable your Computer	√	√	√	√	√	Reflective
	Monitoring your Profiles	√	√	√	√	√	Reflective
	Sent Threatening/Offensive Letter	√	√	√	√	√	Reflective
	Written Menace/Offensive Comments	√	√	√	√	√	Reflective

Note: 1 denotes causal priority between the indicator and the construct; 2 denotes whether the construct is a characteristic or a mixture of indicators that explain the hands. 3 = Do the metrics reflect the construct's effects or causes? 4 = Is it correct that if the trait's appraisal changes, all things will change in the same way (assuming they are all similarly coded)? 5 = Can the objects be swapped out with one another?

Instrument Validity and Reliability (Testing Goodness of Data). Validity and reliability testing are essential in questionnaire construction since a research instrument must be valid and consistent to calculate the study's variables. Validity refers to how well a metric accurately describes the underlying construct it is meant to measure, while reliability refers to how robust or dependable a construct's measure is. A calculation can be accurate but not true, and vice versa. Both reliability and validity are needed to ensure adequate analysis of the constructs of interest [175].

The degree to which a construct's calculation is reliable is known as reliability [175]. Internal continuity, in some terms, evaluates the interrelatedness of items. The scale's items should have a high degree of internal accuracy. Cronbach's coefficient alpha [188] is the most used to calculate the internal accuracy reliability coefficient, and it is concerned with the degree of interrelatedness within a group of objects constructed to measure a single

construct. The higher Cronbach's alpha is, the more reliable the intrinsic stability is. It is considered acceptable if the value is 0.70, but it is appropriate if it is 0.60 or more [177].

The final questionnaire was shown to an additional seven experts. One from UTM was a proofreader (Arabic and English). The others were the dean of the student's college, the deputy dean, and teachers whose purposes were to increase the clarity of the instruction and wording and check the final appearance of the instrument before distributing it. Some researchers suggested that this stage was a pretest of the questionnaire, and their corrections suggested that expert suggestions were affected as well as the content validity.

5. Data Analysis Techniques

Different techniques are used for data analysis depending on the type of statistics used. Three different analyses use survey data: descriptive analysis, measurement model analysis, and structural model analysis.

Descriptive Analysis. Descriptive analysis is the mathematical description, aggregation, and presentation of the structures of interest or relationships [175]. In this report, descriptive analysis was used to examine the respondents' profiles, such as frequency, standard deviation, mean, range, and percentage, using IBM SPSS Statistics 20. The most common data analysis technique for determining relationships between latent variables is structural equation modeling (SEM). It is considered an effective strategy for assessing hypothesized structural linkages between variables and measuring associations between variables and their objects [189]. PLS is a component-based approach to measuring SEM that is often used to model the relationships between dependent and independent variables. The PLS-SEM application has been successfully implemented in various research areas and is becoming widely shared in IS and other disciplines [190]. PLS route modeling can be done using multiple methods, including SmartPLS, used in this analysis. The evaluation of the calculation model and the evaluation of the structural model are all done in the SmartPLS 2.0 method.

Assessment of the Measurement Model. Internal accuracy reliability, indicator reliability, convergent reliability, and discriminant validity are some of the reliability and validity assessments for the reflective measurement model. Table 6 shows the instructions for evaluating the calculation model.

Cronbach's alpha (CA) is a traditional measure of internal accuracy, with a strong alpha value implying that all objects of the same construct have the same range and context [67]. Composite reliability (CR) considers the various outer loadings of the indicator variables, whereas Cronbach's alpha suggests that all indicators are similarly accurate. CA and CR range from 0 to 1, with 0.6–0.7 considered acceptable [191], 0.7–0.9 satisfactory, and values > 0.95 considered unacceptable [179].

The degree to which individual objects represent construct convergence compared to items measuring separate constructs is known as convergent validity [190]. The researchers consider the outer loadings of the metrics with the average variance derived to determine convergent validity (AVE). The lower bound for indicators with external loadings is 0.708, while indicators with external loadings of 0.4 to 0.7 can be deleted only if doing so improves the CR; in the meantime, the value of AVE should be greater than 0.5 for a desirable convergent validity. Finally, discriminant validity, which is characterized as the degree to which a construct is genuinely distinct from other constructs by methodological criteria [179], was used to evaluate reflective constructs in this analysis. To develop discriminant validity in SEM with PLS, two standard measures are used. The first metric is indicator cross-loading, indicating that an indicator's outer loading on the corresponding build should be greater than any other loadings. The Fornell–Larcker criterion, which states that the square root of each construct's AVE should be greater than its highest correlation with any other construct, is the second metric.

Assessment of Structural Model. After the validation of the measurement model, the structural model can be analyzed. Four test criteria were used to assess the structural model, as shown in Table 7.

Table 6. Evaluation of the measurement model [179].

Analysis	Test	Description	Criteria
Internal consistency reliability	Cronbach's alpha (CA)	Based on the intercorrelations of the observed predictor variables, calculate the reliability (all indicators have equal outer loadings).	≥0.6 Acceptable ≥0.7 Satisfactory
	Composite reliability (CR)	Although considering the various outer loadings of the indicator variables, the same (CA) was found.	0.6–0.7 Acceptable 0.7–0.9 Satisfactory >0.95 Redundant
Convergent validity	Indicator reliability (factor outer loading)	Is the square of the outer loading of a standardized predictor. It is referred to as the variance derived from the item and it reflects how much of the difference in an item is described by the construct.	≥0.7 Acceptable
	Average variance extracted (AVE)	The latent construct's ability to describe the variance of its metrics.	≥0.5 Desirable
Discriminant validity	Cross-loadings	An indicator's correlation with other constructs in the model.	Outer loading for a specific construct > its loading on all the other constructs
	Fornell–Larcker criterion	Compares the square root of each construct's average variance derived with all other constructs in the model's correlations.	SQRT (AVE) for each construct > correlation between constructs

Table 7. The assessment of structural model guidelines.

Analysis	Test	Description	Criteria
Coefficient of determination	(R^2)	Measures the relationship of a latent variable to its total variance	0.670 substantia l0.333 moderate 0.190 weak [186]
Path coefficient	(β)	Indicates the strength of the relationship between two latent variables	From −1 to 1. Values closer to 1 are more significant
	t-value		>1.65 significance level 10% >1.96 significance level 5% >2.57 significance level 1%
	p-value		Significant at *p*-value * <0.10 ** <0.05 *** <0.01
Effect size	(f^2)	Measures if an independent latent variable has a substantial impact on a dependent latent variable	$0.02 < f^2 \leq 0.15$ (small effect). $0.15 < f^2 \leq 0.35$ (medium effect). $f^2 > 0.35$ (large effect)
Collinearity issues	Tolerance VIF	Examines each set of predictor constructs separately for each subpart of the structural model	Tolerance > 0.20 acceptable VIF 5 ≥ acceptable
Predictive relevance	Q^2	Indicator of the model's predictive relevance	>0 having predictive relevance
	q^2	The relative impact of predictive relevance (effect size)	0.02 small 0.15 medium 0.35 large

Pilot Testing. After assessing the validation using a theoretical approach, the analytical evaluation is the next step in the validation process. Many refined build elements

are combined into a testing instrument, delivered to a pilot test sample of representative respondents from the target population [175]. A pilot evaluation is a small-scale approximation of the survey execution with representatives of the target community [192]. Pilot testing aims to identify any issues or flaws in the questions (checking that the questions are understandable, answer choices are appropriate, the order of the questions seems logical), the questionnaire layout (font sizes are easy to read, colors and styles), and the questionnaire process (how long it takes respondents to complete answers, how interested the respondents are in the results).

To ensure validity, pilot testing for the current research was conducted after receiving the suggestions and comments from the pretest and content validity procedure [193]. According to Zukerberg et al. [194], few straightforward guidelines exist to determine sample size. Experts' recommendations about the appropriate size cover a substantial range, which is considered in the current study. Sudman [195] mentioned that a pilot test on 20–50 cases is sufficient, and Sim and Lewis [196] stated that a pilot study of at least 50 cases was advisable in many circumstances, while the range may vary from 25 to 100 subjects [197]. Thabane et al. [198] stated that sample size calculation might not be required for some studies in general. To accomplish the pilot survey task, 50 questionnaires were distributed. Based on the data collected from the pilot study, descriptive analysis was performed, followed by validation of the instrument's reliability (see Tables 8 and 9 for descriptive analysis and reliability).

Table 8. Respondents' demographic characteristics.

Var.	Items	Freq.	%	Var.	Items	Freq.	%
Gender	Male	31	62	Nationality	Local	43	86
	Female	19	38		Foreigner	7	14
Age	Fewer than 18	0	0	Academic semester	First sem.	9	18
	18	1	2		Second sem.	18	36
	19	6	12		Third sem.	5	10
	20	14	28		Fourth sem.	8	16
	21	14	28		Fifth sem.	6	12
	22	10	20		Sixth sem.	4	8
	Others	5	10	Income	Fewer than 500	15	30
Course program	Engineering	24	48		500–749	11	22
	Computer sci./IT	1	2		750–999	5	10
	Applied Arts	6	12		1000–1500	10	20
	Finance and Management	10	20		More than 1500	8	16
	Medical Sciences	6	12		Others	1	2
	Education	0	0	Residency	City	47	94
	Languages	0	0		Rural	0	0
	Hotel and Tourism	1	2		Refugee	2	4
	Audio and Visual Techniques	0	0		Desert	0	0
	Information Management and Libraries	2	4		Town	1	2
	Others	0	0		Village	0	0

Table 9. Reliability analysis of pilot study.

Construct	Number of Items	Cronbach's Alpha
Proximity to motivated offender	23	0.781
Suitable target	12	0.723
Digital guardianship	12	0.751
Cyberstalking	8	0.768

Data Collection. After assessing the reliability and validity of the questionnaire, copyright was applied from the Innovation and Commercialization Centre (ICC) at UTM. This was successful in December 2015 with the awarding of copyright labeled: Survey on Cyberstalking victimization <2015> Universiti Teknology Malaysia—All rights reserved.

Descriptive Analysis of Pilot Study. The overall number of respondents that participated in the pilot study was 50. IBM SPSS statistics 20 was used to exhibit the respondents' demographic characteristics in this study. The frequencies and percentages are shown in Table 8.

Instrument's Reliability. The reliability of the device was evaluated using Cronbach's alpha. The results showed that all variables have an acceptable level of reliability, with all the scales being reliable at >0.70 (see Table 9).

6. The Theoretical Framework Concept

The tenets of routine activities and lifestyle exposure theories have been combined to create what is known as L-RAT [48,82,83]. This combination is implicit in lifestyle routine activity theories, lifestyle exposure theory, and routine activities theory used interchangeably in research such as Reyns [36]. The two separate approaches were developed in tandem and shared scientific ideas [83,199]. Although the L-RAT perspective has been applied to various physical crimes, its application to cybercrime is limited. The theoretical integration is essential in helping to explain the new crime phenomenon [77,93]. The L-RAT perspective has been one of the most tried and supported analytical models [83,99]. Cyberstalking as a new phenomenon of cybercrime has not been extensively empirically examined [32]. Only a few observational trials have been conducted, and most cyberstalking studies lack a scientific basis [65,82]. Recently, researchers have used this perspective to conduct studies about cyberstalking victimization [24]. This study proposes a conceptual model for this new phenomenon to cover the dire need for empirical assessment of cyberstalking victimization based on the L-RAT perspective. The conceptual model describes the theoretical framework and helps the reader visualize the theorized relationships [177]. The conceptual model of this study consists of four variables: proximity to motivated offenders, suitable target (target attractiveness, digital guardianship and cyberstalking victimization, moderators, and demographic/control variables).

In prior studies, researchers used the term "proximity" or "exposure" interchangeably. The proximity to motivated offender variable for this study was operationalized using 23 items: hacking, political websites, e-banking, showing goods and services, job-seeking websites, e-government, health-care services, chatting/instant messenger (video), chatting/instant messenger (voice), chatting/instant messenger (text), social networking sites, sending/receiving emails, reading newspapers/magazines, playing games, watching TV programs, downloading computer programs, watching/downloading movies, listening to/downloading music, visiting religious websites, shopping, visiting adult websites, sport, adding unknown friend (see Figure 4). To assess the suitable target variable, 12 items were operationalized, including the victims' personal information that was exhibited on the Internet: name, gender, age, mobile phone number, email address, home address, bank account number, study program, credit card serial, favorite activities, photos, videos (see Figure 5). The guardianship variable was operationalized using 12 items, including the security software installation that the victims frequently activated: antivirus software, antispyware software, firewall software, Ad-Aware software, tracking protection blocks software, filtering/monitoring software (see Figure 6). The information security management techniques that the victims frequently used on their computers were also included: change the login password, save extra copies from files/folders, create a backup process, delete old files, delete old emails/attachments, change any file locations.

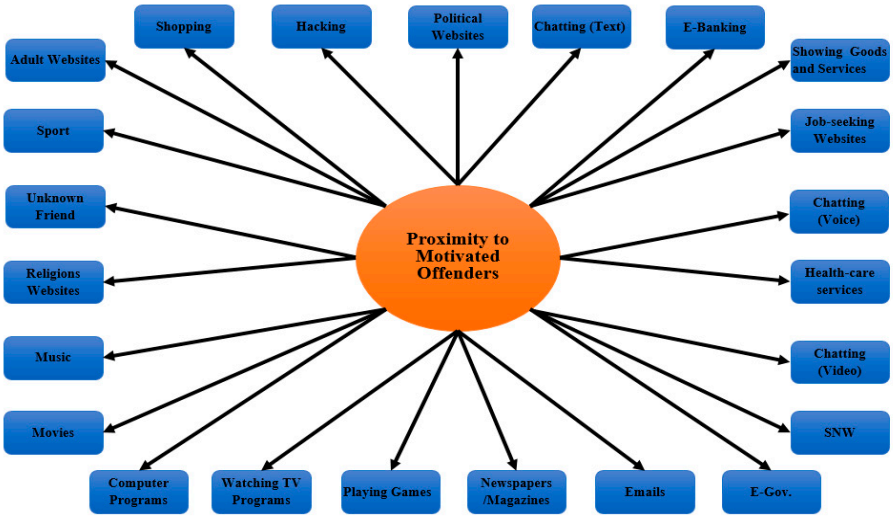

Figure 4. Proximity to motivated offender model.

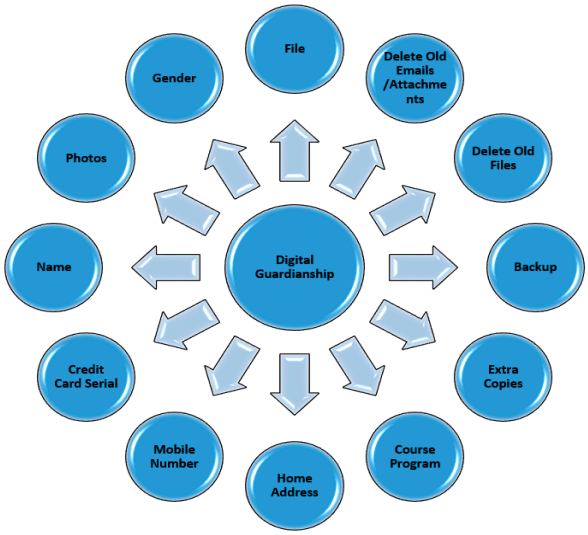

Figure 5. Suitable target model.

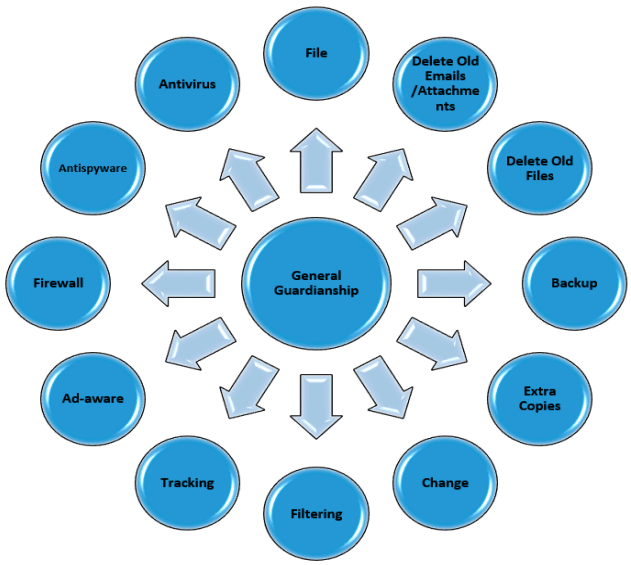

Figure 6. Digital guardianship model.

Seven control variables were assessed for this study: age (less than 18, 18, 19, 20, 21, 22, others), course program (engineering, computer sciences/it, applied arts, finance and management, medical sciences, education, languages, hotel and tourism, audio and visual techniques, information management and libraries, others), academic semester (first, second, third, fourth, fifth, sixth semester), nationality (Jordanian, foreigner), residence (village, desert, rural, refugees, town, city, other), gender (male, female) and income (less than 500, 500–749, 750–999, 1000–1499, more than 1500 Jordan Dinars, others). The only dependent variable in the current study was operationalized using eight items by asking the victims about the online victimization behavior that they frequently faced, including being harassed or annoyed, having false information posted, being sent sexual material, someone pretending to be them, attempts to disable their computer, having their online profile monitored, being sent threatening/offensive letters or messages to their e-mail, having threatening/offensive comments made to them in chat rooms/on instant messaging sites (see Figure 7). A proposition is a "tentative and conjectural association between constructs", and "hypotheses" refer to the analytical formulation of these propositions as relationships between variables [175]. With a few exceptions, comprehensive reviews of the L-RAT perspective for cyberstalking victimization lack literature. Most experiments have not operationalized any theory's ideas (proximity to a motivated criminal, appropriate goal (target attractiveness), and digital guardianship). To account for cyberstalking victimization, this analysis thoroughly examined all of the theory's ideas, and all hypotheses were formulated as follows:

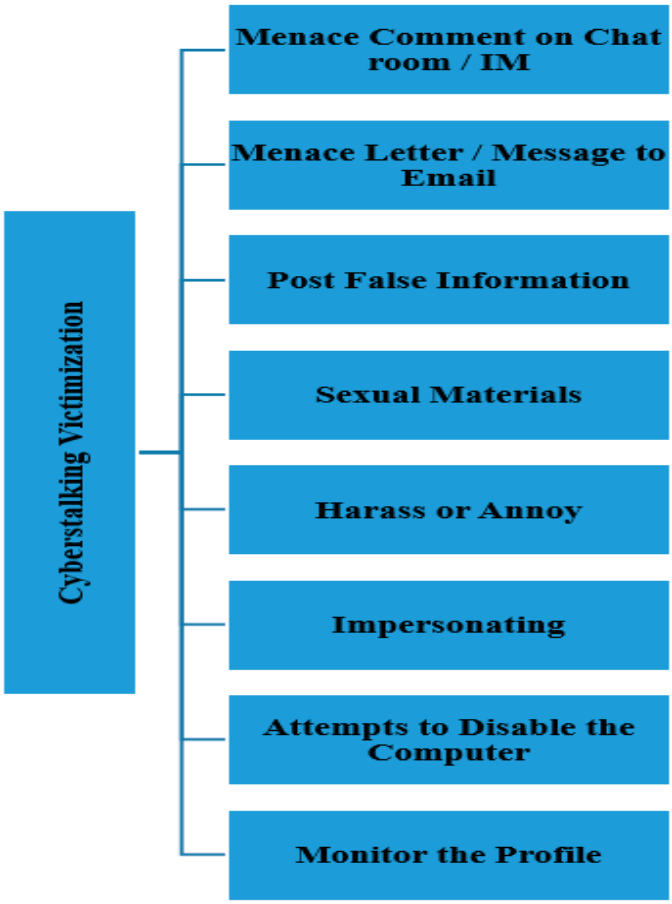

Figure 7. Cyberstalking victimization model.

Hypothesis 1 (H1). *Proximity to motivated offender has a positive effect on cyberstalking victimization.*

Hypothesis 2 (H2). *Suitable target has a positive effect on cyberstalking victimization.*

Hypothesis 3 (H3). *Digital guardianship harms cyberstalking victimization.*

Due to the disparities between people's diets, lifestyle sensitivity theory, which indirectly included the L-RAT viewpoint, claimed differences in victimization rates across demographic classes. Age, sex, race, marital status, wealth, education, and profession all affected people's lifestyles [48,99]. Five moderators tested the impact of the interaction between the independent variables (proximity to driven attacker, appropriate goal (target attractiveness), and digital guardianship) and the dependent variable (cyberstalking victimization) to thoroughly assess the L-RAT and deliver/answer the study question about the demographic effects on cyberstalking victimization (cyberstalking victimization). The following are the fifteen theories that were proposed:

Hypothesis 4a (H4a). *The relationship between proximity to motivated offenders and cyberstalking victimization is moderated by gender.*

Hypothesis 4b (H4b). *The relationship between suitable target and cyberstalking victimization is moderated by gender.*

Hypothesis 4c (H4c). *The relationship between digital guardianship and cyberstalking victimization is moderated by gender.*

Hypothesis 5a (H5a). *The relationship between proximity to motivated offenders and cyberstalking victimization is moderated by age.*

Hypothesis 5b (H5b). *The relationship between suitable target and cyberstalking victimization is moderated by age.*

Hypothesis 5c (H5c). *The relationship between digital guardianship and cyberstalking victimization is moderated by age.*

Hypothesis 6a (H6a). *The relationship between proximity to motivated offenders and cyberstalking victimization is moderated by Internet speed.*

Hypothesis 6b (H6b). *The relationship between suitable target and cyberstalking victimization is moderated by Internet speed.*

Hypothesis 6c (H6c). *The relationship between digital guardianship and cyberstalking victimization is moderated by Internet speed.*

Hypothesis 7a (H7a). *The relationship between proximity to motivated offenders and cyberstalking victimization is moderated by residence.*

Hypothesis 7b (H7b). *The relationship between suitable target and cyberstalking victimization is moderated by residence.*

Hypothesis 7c (H7c). *The relationship between digital guardianship and cyberstalking victimization is moderated by residence.*

Hypothesis 8a (H8a). *The relationship between proximity to motivated offenders and Cyberstalking victimization is moderated by nationality.*

Hypothesis 8b (H8b). *The relationship between suitable target and Cyberstalking victimization is moderated by nationality.*

Hypothesis 8c (H8c). *The relationship between digital guardianship and cyberstalking victimization is moderated by nationality.*

7. Results of Data Analysis

7.1. Data Collection

Data collection challenges must be resolved after the data is collected and before the analysis: incomplete data, suspicious response habits consisting of straight-lining or contradictory responses, and outlines. Missing data occurs when a respondent fails to answer more than one question, either deliberately or accidentally. Where the percentage of missing data in a questionnaire exceeds 15%, the result is usually disconnected. Mean value substitution was used to handle missing values in this analysis, captured by SmartPLS tools. The mean of the correct values of the indicator variable was used to replace the missing value of the indicator variable. Another problem with the data gathered is the straight-lining, which happens when a respondent answers many questions. Outliers have a solid solution to a single question or have drastic answers to all questions, in the straight-lining issue, the respondent cases should be removed, and in the outlier issue, if there are few identified outlier cases, the respondent cases are removed from the data set [179]. Consequently, over 908 questionnaires were distributed to the replacements, and 757 questionnaires were eligible for analysis, which meant that 151 cases were removed from the data set (see Table 10).

Table 10. Survey summary.

NO.	Description	N	%
1	Questionnaires distributed	908	100
2	Questionnaires received	908	100
3	Incomplete questionnaire (missed data)	104	11.5
4	Suspicious response patterns (straight-lining)	40	4.4
5	Outliers	7	0.77

As shown in Table 10, the response rate of the questionnaire was 100%, which means that all questionnaires were returned. The questionnaires with a high level of missing data were deleted from the data set (11.5%, N = 104). All straight-lining was removed (4.4%, N = 40). Finally, the few outliers were removed (0.77%, N = 7). Descriptive statistics exhibit the essential characteristics feature of the study sample. IBM SPSS Statistics 20 software was used to analyze the descriptive statistics. Table 11 shows the frequencies and percentages of the demographic variables: gender, age, course program, academic semester, nationality, income, and place of residence (see Table 11).

The college students in the case study had to be 18 or more than 18 years, there were 25 respondents aged 18 (3.3%), 70 respondents aged 19 (9.2%), 209 respondents aged 20 (27.6%), 237 respondents aged 21 (31.3%), 165 respondents aged 22 (21.8%), 13 respondents aged 23 (1.7%), 14 respondents aged 24 (1.8%), 7 respondents aged 25 (0.9%), 2 respondents aged 26 (0.3%), 6 respondents aged 27 (0.8%), 2 respondents aged 28, 29, and 30 (0.3%) for each age, 1 respondent aged 33, 38, and 40 (0.1%) for each age. The course program variable comprised of 10 categories: applied arts comprised 72 cases (9.5% of the respondents), audio and visual techniques comprised 28 cases (3.7% of the respondents), computer science/information technology comprised 15 cases (2.0% of the respondents), education comprised 25 cases (3.3% of the respondents), engineering comprised 304 cases (40.2% of the respondents), finance and management comprised 101 cases (13.3% of the respondents), hotel and tourism comprised 61 cases (8.1% of the respondents), information management and libraries comprised 35 cases (4.6% of the respondents), languages comprised 25 cases (3.3% of the respondents), finally medical

sciences comprised 91 cases (12.0% of the respondents).The academic semester variable comprised of six categories: first semester comprised 85 cases (11.23% of the respondents), second semester comprised 149 cases (19.7% of the respondents), third semester comprised 96 cases (12.7% of the respondents), fourth semester comprised 229 cases (30.3% of the respondents), the fifth semester comprised 125 cases (16.5% of the respondents), finally the sixth semester comprised 73 cases (9.6% of the respondents). The nationality variable is comprised of two categories: local and foreigner. The local (Jordanian) category comprised 698 and the foreigners 59 (92.2% and 7.8%, respectively). The income variable comprised of five categories: family monthly income less than 500 Jordanian dinars comprised 252 cases (33.3% of the respondents), 500–749 Jordanian dinars comprised 160 cases (21.1% of the respondents), 750–999 Jordanian dinars comprised 136 cases (18.0% of the respondents), 1000–1499 Jordanian dinar comprised 96 cases (12.7% of the respondents), finally more than 1500 comprised 112 cases (14.8% of the respondents). Place of residence variable shaped by six categories: city comprised 510 cases (67.4% of the respondents), desert comprised 22 cases (2.9% of the respondents), refugee comprised 65 cases (8.6% of the respondents), rural comprised 25 cases (3.3% of the respondents), the town comprised 53 cases (70% of the respondents), finally village comprised 82 cases (10.8% of the respondents).

Table 11. Descriptive demographic statistics.

Var.	Items	Freq.	%	Var.	Items	Freq.	%
Gender	Male	367	48.5	Nationality	Local	698	92.2
	Female	390	51.5		Foreigner	59	7.8
Age	Fewer than 18	0	0	Academic semester	First sem.	85	11.2
	18	25	3		Second sem.	149	19.7
	19	70	9		Third sem.	96	12.7
	20	209	28		Fourth sem.	229	30.3
	21	237	31		Fifth sem.	125	16.5
	22	165	22		Sixth sem.	73	9.6
	Others	51	7	Income	Fewer than 500	225	33.3
Course program	Engineering	304	40.2		500–749	160	21.1
	Computer Sci./IT	15	2		750–999	136	18
	Applied Arts	72	9.5		1000–1500	96	12.7
	Finance and Management	101	13.3		More than 1500	113	14.9
	Medical Sciences	91	12		Others	1	2
	Education	25	3.3	Residency	City	510	67.4
	Languages	25	3.3		Rural	25	3.3
	Hotel and Tourism	61	8.1		Refugee	65	8.6
	Audio and Visual Techniques	28	3.7		Desert	22	2.9
	Information Management and Libraries	35	4.6		Town	53	7
	Others	0	0		Village	82	10.8

The first objective of the current study is to estimate the prevalence of this new phenomenon among college students. To achieve this objective, IBM SPSS Statistics 20 was employed to calculate the percentages across the eight categories of cyberstalking victimization behaviors that were defined. The behaviors consist of harassment or annoyance, posting false information, sending sexual material, pretending to be you, attempting to disable a computer, monitoring your profile, sending threatening letters or messages to your email, writing threatening/offensive comments to you in chat rooms/on instant messaging sites. Table 12 shows the percentage of prevalence for each type of cyberstalking victimization.

Table 12. Cyberstalking victimization prevalence.

Cyberstalking Victimization Behavior Type				Prevalence
Type	**Likert Value**	**Frequency**	**%**	**The Calculation Used the Weighted Average [1]**
Harassment/annoyance	1	93	12.3	66.76%
	2	122	16.1	
	3	167	22.1	
	4	189	25.0	
	5	186	24.6	
Posted false information about you	1	359	47.4	39.92%
	2	223	29.5	
	3	49	6.5	
	4	74	9.8	
	5	52	6.9	
Sent sexual materials to you	1	138	18.2	64.64%
	2	124	16.4	
	3	88	11.6	
	4	239	31.6	
	5	168	22.2	
Pretended to be you without your permission	1	137	18.1	60.00%
	2	187	24.7	
	3	115	15.2	
	4	175	23.1	
	5	143	18.9	
Attempted to disable your computer	1	212	28.0	57.20%
	2	138	18.2	
	3	80	10.6	
	4	198	26.2	
	5	129	17.0	
Monitored your profile online	1	140	18.5	61.30%
	2	169	22.3	
	3	98	12.9	
	4	199	26.3	
	5	151	19.9	
Sent threatening/offensive letters or messages to your e-mail	1	142	18.8	64.84%
	2	49	6.5	
	3	214	28.3	
	4	189	25.0	
	5	163	21.5	
Wrote threatening/offensive comments to you in chat rooms/IMs	1	256	33.8	49.18%
	2	158	20.9	
	3	152	20.1	
	4	121	16.0	
	5	70	9.2	

[1] Sum ((value∗percentage)/100)/5)∗100%.

As shown in Table 12, the cyberstalking victimization prevalence ranged between 66.76% (harassment and annoyance) and 39.92% (posted false information). In addition, 64.64% of students received sexual materials, 57.2% had their computers disabled, 61.3% had their profile monitored online, 64.84% were sent threatening letters or messages to their email, 49.18% were sent threatening/offensive comments in chat rooms/on instant messaging sites, and finally, 60% were impersonated.

7.2. Model Quality Assessment

System validation attempts to determine whether the structural model and calculation meet the consistency standards for analytical work [190]. According to Hair et al. [179], this point focuses on learning how to evaluate the consistency of the performance. The evaluation of the structural model (inner model) and the assessment of the estimation models are the two steps in the formal application of these parameters (outer models). The structural equation model is developed by combining the calculation and structural models.

Assessment of the Measurement Models (Outer Models). It is essential to decide whether the measurement paradigm is reflective or formative before assessing it. The current study's model was reflective. Composite reliability is used to test internal accuracy, predictor consistency, average variance derived (AVE) to assess convergent validity, and cross-loading, and the Fornell–Larcker criteria to determine discriminant validity [179].

Convergent Validity. The degree to which a metric compares positively with alternative measurements of the same construct using the domain sampling model; reflective construct metrics are viewed as separate ways to measure the same construct. Hair et al. [179] identified convergent validity. As a result, objects that are indices (measures) of a particular construct should converge or have a high proportion of variation in common. Convergent validity is noted when things that seem to represent a concept combine, or exhibit major, high similarities with one another, according to Straub et al. [200]. The degree to which several construct metrics agree with one another is known as convergent validity [201]. As a result, according to Hair et al. [179], convergent validity can be assessed using outer loadings and average variance removed (AVE).

Outer Loadings. In reflective calculation models, outer loadings are the approximate relationships that specify an item's total contribution to its assigned build. Its value should be greater than 0.70, according to Hair et al. [179], but if it is between 0.4 and 0.7, there are certain things to remember when removing the object from the scale. Other research, however, determined that 0.50 was the minimum cut-off value for keeping the object on the scale [189,202–204]. Thus, things with values of 0.50 and above were compatible with previous research and were suggested to be held (see Table 13 for the retaining indicators).

Average Variation Extracted (AVE). The degree to which a latent construct enlightens the variance of its respective indicators is measured by AVE. The build clarifies more than half of the uncertainty of its indicators if the AVE value is 0.50 or higher [179]. The AVE values for this analysis are shown in Table 13.

Table 13. Convergent validity.

Construct	Indicators	Outer Loading	AVE
PTMO	Adding unknown friend	0.6710	0.5478
	Chatting/instant messenger (text)	0.7280	
	Chatting/instant messenger (voice)	0.5676	
	Playing games	0.8233	
	Reading newspapers/magazines	0.7993	
	Sending/receiving emails	0.8319	
	Social networking sites	0.7819	
	Visiting religious websites	0.8236	
	Watching/downloading movies	0.6518	
	Listening to/downloading music	0.6730	
ST	Mobile phone number	0.5540	0.5765
	Home address	0.7986	
	Bank account number	0.8684	
	Videos	0.7067	
	Photos	0.7524	
	Name	0.6207	
	Gender	0.7662	
	Email Address	0.8582	
	Age	0.8460	

Table 13. *Cont.*

Construct	Indicators	Outer Loading	AVE
DG	Ad-Aware software	0.8298	0.6353
	Antispyware software	0.7580	
	Antivirus software	0.7910	
	Filtering/monitoring software	0.7753	
	Firewall software	0.7942	
	Tracking Protection blocks software	0.8390	
	Change any file locations	0.7361	
	Delete old emails/attachments	0.8301	
	Login password	0.8136	
CV	Attempted to disable your computer	0.7824	0.5541
	Monitored your online profiles	0.8147	
	Pretended to be you online without your permission	0.8637	
	Sent sexually explicit materials to you	0.5594	
	Sent threatening/offensive letters or messages to your e-mail	0.6599	

Discriminant Validity. The discriminant validity denotes the clarity of the construct components [201,205]. Straub et al. [200] defined discriminant validity as the posited of the measurement items to show ("makeup") that construct vary from those which are not assumed to form the construct. In line with these definitions, according to Hair et al. [179], discriminant truth is "the degree to which one concept is completely distinct from other constructs by scientific criteria." Cross-loadings and the Fornell–Larcker criteria are two techniques for determining discriminant validity. One tool for determining discriminant validity is cross-loadings. Explicitly, an indicator's outer loading on the corresponding build should be greater than any other loadings. Another way of evaluating discriminant validity is the Fornell–Larcker criteria [206], which assumes that AVE should be greater than the construct's highest squared correlations with other latent constructs. Consequently, since the current study model consists of four constructs only (relatively small) with more items, it is recommended to use the cross-loadings method because it depended on the individual items in the comparison, so cross-loadings were used (see Table 14).

Internal Consistency Reliability. The customary criterion for evaluating internal consistency reliability is Cronbach's alpha (CA), which supposes reliability of all indicators, while composite reliability (CR) considers that indicators show dissimilar loadings [190,207]. CA and CR differ between 0 and 1 respectively, with greater values that show a higher level of reliability. An alpha coefficient value of 0.7 is measured well; an acceptable value for some researchers, such as Sekaran and Bougie [177], is between 0.6 and 0.7. Table 15 exhibits the values of CA and CR for the constructs used in the current study with all the values for CA, which range from 0.793 to 0.928 and 0.859 to 0.923. The results show that all the items are reliable.

Assessment of the Structural Model (Inner Model). Hence it is proven that the measurement model defines the construct (latent variables), while the structural model explains the underlying causative relationship among these latent variables [189]. This specifies that after the confirmation, it is a helpful fact that the construct measures are consistent and dependable. By this, the structural model can be assessed [177,179,204]. The assessment of the structural model can be achieved by applying the following tests under specified criteria: first: coefficient of determination (R^2); secondly: f^2 effect size test; thirdly, predictive relevance of the model (Q^2) and (q^2) effect size; finally, measuring the relevance and significance of the structural model utilizing path coefficient and standard errors (*t*-value) through the bootstrapping procedure [179,190,204].

The Coefficient of Determination (R^2 value). Hair et al. [179] stated that R^2 value is "a measure of the model's suggestive correctness, and it is measured as a squared connection between actual and predicted values of a specific endogenous construct. The coefficient signifies the endogenous latent variable's collective effects on the endogenous

latent variable; it also shows the amount of variance in the endogenous construct clarified by all the exogenous constructs linked to it."

Table 14. Cross-loading discriminant validity.

Indicators	PTMO	ST	DG	CV
PTMO01	0.6518	0.5911	0.5501	0.5636
PTMO02	0.8236	0.7535	0.7173	0.7140
PTMO03	0.7819	0.7660	0.7393	0.7174
PTMO04	0.8319	0.7815	0.7126	0.6708
PTMO05	0.7993	0.7262	0.7890	0.7666
PTMO06	0.8233	0.7503	0.6746	0.7508
PTMO07	0.5676	0.5635	0.5645	0.4354
PTMO08	0.7280	0.6690	0.6359	0.6513
PTMO09	0.6710	0.6329	0.6013	0.4842
PTMO10	0.6730	0.5955	0.5856	0.4658
ST01	0.5178	0.5540	0.5044	0.3782
ST02	0.7386	0.7986	0.7557	0.6857
ST03	0.8274	0.8684	0.7723	0.7497
ST04	0.5951	0.7067	0.6191	0.5598
ST05	0.6533	0.7524	0.6559	0.6091
ST06	0.5782	0.6207	0.6179	0.5231
ST07	0.7654	0.7662	0.6982	0.7388
ST08	0.7758	0.8582	0.7468	0.7155
ST09	0.8115	0.8460	0.8236	0.7478
DG01	0.6542	0.6460	0.7361	0.6514
DG02	0.7645	0.7307	0.7942	0.6795
DGO3	0.7009	0.7157	0.7753	0.6879
DG04	0.7514	0.7934	0.8390	0.7114
DG05	0.6865	0.7417	0.8301	0.7173
DG06	0.7104	0.7183	0.7910	0.6907
DG07	0.6744	0.7196	0.7580	0.6805
DG08	0.7893	0.7893	0.8298	0.6609
DG09	0.6723	0.7073	0.8136	0.6740
CV01	0.6896	0.6790	0.6382	0.7824
CV02	0.7573	0.7252	0.7704	0.8147
CV03	0.7498	0.7025	0.7280	0.8637
CV04	0.4270	0.5084	0.5124	0.5594
CV05	0.4975	0.5193	0.4939	0.6599

Table 15. Internal consistency reliability.

Construct Alpha	Cronbach's Alpha (CA)	Composite Reliability (CR)
PTOM	0.907	0.923
ST	0.905	0.923
DG	0.928	0.940
CV	0.793	0.859

The range of R^2 value is from 0 to 1 with a higher level which shows higher levels of predictive accuracy. The judgment of R^2 level as high depends on the research disciplines and model complexity, whereas R^2 values of 0.2 are measured high in specific disciplines, such as consumer behaviors. Values of approximately 0.67, 0.3330, and 0.19 are considered substantial, moderate, and weak, respectively [186,190,207], whereas familiar scholars and researchers consider R^2 values of 0.750, 0.500, and 0.250 substantial, moderate, and weak, respectively. The R^2 value of the endogenous latent variable (cyberstalking victimization (CV)) is 0.782, which means that the influence of proximity is 78.1% of the variance in the CV, which indicates a substantial range.

Effect Size (f^2). The change of these values can be explored, besides the evaluation of R^2 values, to identify whether the effect of a particular independent latent variable on a

latent dependent variable has a substantive e-impact [179,190,204,207]. The effect size f^2 can be calculated as:

$$f^2 = \frac{R^2_{included} - R^2_{excluded}}{1 - R^2_{included}} \quad (1)$$

When the predictor latent variable is used or omitted in the structural equation, $R^2_{included}$ and $R^2_{excluded}$ are the R^2 given on the latent dependent variable, respectively [204]. Thus, at the structural stage, values of 0.020, 0.150, and 0.350 can be used to determine whether a latent predictor variable has a small, medium, or strong effect [179,190,204,207]. Table 16 exhibits the result of the effect size test.

Table 16. Effect size (f^2) of latent variables.

Path (R^2 = 0.728)	$R^2_{excluded}$	Effect Size (f^2)	Rating
PTMO→CV	0.765	0.078	Small effect
ST→CV	0.780	0.009	Very small effect
DG→CV	0.760	0.101	Small effect

PTMO = Proximity to motivated offenders, ST = suitable target, DG = digital guardianship, CV = cyberstalking victimization.

From the results, $f^2_{PTMO→CV}$ = 0.078, $f^2_{ST→CV}$ = 0.009 and $f^2_{DG→CV}$ = 0.101 had a small effect on CV. The completed formula results are as follows:

$$f^2_{PTMO→CV} = \frac{R^2_{included} - R^2_{excluded}}{1 - R^2_{included}} = 0.782 - 0.765/1 - 0.782 = 0.078. \quad (2)$$

$$f^2_{SU→CV} = \frac{R^2_{included} - R^2_{excluded}}{1 - R^2_{included}} = 0.782 - 0.780/1 - 0.782 = 0.009. \quad (3)$$

$$f^2_{DG→CV} = \frac{R^2_{included} - R^2_{excluded}}{1 - R^2_{included}} = 0.782 - 0.760/1 - 0.782 = 0.101. \quad (4)$$

Predictive Relevance (Q^2). Predictive relevance is a method to evaluate the magnitude of the R^2 values as a criterion of predictive accuracy by using Stone–Geisser's Q^2 [208,209].

In SmartPLS 2.0, blindfolding technique is available as built-in software. Two contemplations must primarily be considered as basics to run the blindfolding procedure: firstly, this procedure is applicable only for both reflective and single-item constructs, respectively; further, it should be determined which data points are deleted (omitted) by setting an omission distance (D). D should be chosen between 5 and 10 [179]. In the current study, D was set automatically by the software to 7 (as default). Q^2 is calculated as follows:

$$Q^2 = \frac{1 - SSE}{SSO} \quad (5)$$

Q^2 = predictive relevance, SSE = sum of squared predictive errors, and SSO = sum of squared observations.

For predictive quality and relevance, the Q^2 value must be more than zero. After running the blindfolding procedure, the construct cross-validated redundancy result shows that the Q^2 value is 0.4267, reflecting an excellent predictive relevance for cyberstalking victimization. The subsequent phase was to assess the predictive relevance for each independent variable alone to predict cyberstalking victimization, which refers to q^2 using the following formula:

$$q^2 = \frac{Q^2_{included} - Q^2_{excluded}}{1 - Q^2_{included}} \quad (6)$$

where, q^2 is effect size of predictive relevance. $Q^2_{included}$ and $Q^2_{excluded}$: the predictive relevance value for the endogenous latent variable when the exogenous latent variable is used or omitted, where values of 0.02, 0.15, and 0.35 assume that the effect size for predictive relevance is small, medium, and large, respectively (see Table 17).

Table 17. Predictive relevance of latent variables.

Path (Q^2 = 0.4267)	$Q^2_{excluded}$	Effect Size (q^2)	Effect
PTMO→CV	0.4188	0.014	Small
ST→CV	0.4265	0.0004	Small
DG→CV	0.4166	0.018	Small

PTMO = proximity to motivated offenders, ST = suitable target, DG = digital guardianship, CV = cyberstalking victimization.

As shown in Table 17, the results obtained from calculations are as follows:

$$q^2{}_{PTMO\rightarrow CV} = \frac{Q^2{}_{included} - Q^2{}_{excluded}}{1 - Q^2{}_{included}} = 0.4267 - 0.4188/1 - 0.4267 = 0.014. \quad (7)$$

$$q^2{}_{SU\rightarrow CV} = \frac{Q^2{}_{included} - Q^2{}_{excluded}}{1 - Q^2{}_{included}} = 0.4267 - 0.4265/1 - 0.4267 = 0.0004. \quad (8)$$

$$q^2{}_{DG\rightarrow CV} = \frac{Q_{included} - Q^2{}_{excluded}}{1 - Q^2{}_{included}} = 0.4267 - 0.4166/1 - 0.4267 = 0.018. \quad (9)$$

Hypotheses Testing (Path Coefficient and Bootstrapping). After running the PLS–SEM algorithm, the path coefficient obtained from the structural model relationships represented the hypothesized relationships among the constructs. Several algorithms can be used to determine the model structure [210–215]. The path coefficients show a standardized value ranging from −1 to 1+. A robust positive relationship implies that the path coefficient value is close to +1 and vice versa for close to −1. The standard error depends on the significance of the coefficient, which is achieved utilizing bootstrapping. The standard bootstrapping error makes the empirical *t*-value to be calculated. Before doing the bootstrapping in SmartPLS 2.0, the samples were set to 5000, the R^2 for cyberstalking victimization (the only dependent variable) for the current study was 0.781, and there are commonly critical values used to compare it with *t*-value to test the significance level. These were 1.650 (with 10% of significance level), 1.960 (with 5% significance level) and 2.580 (with 1% significance level).

H1 hypothesized that proximity to motivated offenders has a significant positive effect on cyberstalking victimization. The results demonstrated a significant and positive effect of proximity to motivated offenders on cyberstalking victimization (path coefficient = 0.3721, STERR = 0.0641, *t*-value = 5.8085 *** > 2.58, $p < 0.01$). The results showed that PTMO was statistically significantly related to cyberstalking victimization, and therefore, H1 was accepted. H2 hypothesized that a suitable target has a significant positive effect on cyberstalking victimization. The results demonstrated a significant and positive effect of ST on cyberstalking victimization (path coefficient = 0.1547, STERR = 0.0797, *t*-value = 1.9423 * > 1.65, $p < 0.1$). The results showed that SU was statistically significantly related to cyberstalking victimization, and therefore, H2 was accepted. H3 hypothesized that digital guardianship has a significant negative effect on cyberstalking victimization. The results demonstrated a highly significant and positive effect of digital guardianship on cyberstalking victimization (path coefficient = 0.3848, STERR = 0.0600, *t*-value = 6.4162 > 2.58 ***, $p < 0.01$). The results exhibited that DG was statistically significantly related to cyberstalking victimization but with a positive relationship.

A moderator effect occurs when an independent variable changes the strength of a relationship in the model between two constructs. There are two types of moderating relationships, categorical and continuous. Categorical moderating effects occur with a categorical variable that affects all relationships, which commonly came with two choices such as, gender (male or female). Continuous moderating effects, on the other hand, happen when a non-categorical variable affects a relationship in a model. The researchers often transform the continuous variable into a categorical variable to model its unique effect on the relationship as continuous [179]. Consequently, this study employed the categorical moderators' type to assess the significance of moderating effects for five variables (gender,

nationality, Internet speed, age, and residence) from exogenous latent variables (IV) to endogenous latent variables (DV).

The first categorical moderating effect was assessed using the parametric approach to PLS multigroup (MGA). MGA is a multigroup analysis technique and was used to test differences between identical models estimated for different groups of data [179]. The parametric approach, as proposed by Keil et al. [216], requires three parameters to be specified: The number of observations in the first group n (1) and in the current test (male or female) were referred to as n (2). The two groups' path coefficients were referred to as *p* (1) and *p* (2). The standard errors of the parameter for the groups, which were referred to as (*p* (1)) and (*p* (2)) (see Table 18).

Table 18. PLS-MGA results for the gender moderating effect.

Exogenous Latent Variables	Male		Female		Male vs. Female		
	p(1)	se(*p(1)*)	*p(2)*	se(*p(2)*)	$\lvert p(1) - p(2) \rvert$	*t*-Value	*p*-Value
PTMO→CV	0.414	0.0723	0.350	0.0580	0.064	0.695	0.487
ST→CV	0.092	0.0867	0.205	0.0731	0.113	1.002	0.317
DG→CV	0.401	0.0583	0.363	0.0588	0.038	0.459	0.646
N	367		390		-	-	-

PTMO = proximity to motivated offenders, ST = suitable target, DG = digital guardianship, CV = cyberstalking victimization.

As shown in Table 18, the path coefficients and standard errors showed little difference. The highest variance in path coefficient was observed in the relation between suitable target and cyberstalking (0.113). However, the *t*-value = 1.002 and *p*-value = 0.317 indicated no statistical significance for the effect of gender on any exogenous latent variables. Therefore, it was concluded that gender is not a moderator between PTMO, ST, and DG and the endogenous latent variable (CV). The same method was conducted in the nationality variable with the indicators local (Jordanian) and foreigner. A PLS-MGA analysis was performed to test the nationality moderating effect between PTMO, ST, and DG) and CV (see Table 19).

Table 19. PLS-MGA results for the nationality moderating effect.

Exogenous Latent Variables	Local		Foreigner		Local vs. Foreigner		
	p(1)	se(*p(1)*)	*p(2)*	se(*p(2)*)	$\lvert p(1) - p(2) \rvert$	*t*-Value	*p*-Value
PTMO→CV	0.382	0.0644	0.307	0.0593	0.0753	0.366	0.715
ST→CV	0.125	0.0809	0.391	0.0458	0.2663	1.033	0.302
DG→CV	0.404	0.0606	0.238	0.0490	0.1654	0.855	0.393
N	598		59		-	-	-

PTMO = proximity to motivated offenders, ST = suitable target, DG = digital guardianship, CV = cyberstalking victimization.

As shown in Table 19, the highest variance in path coefficient was observed in the relation between ST and CV (0.2663). However, the *t*-value = 1.033 and *p*-value = 0.302) indicated no statistical significance for the effect of nationality on any exogenous latent variables. Therefore, it was concluded that nationality is not a moderator between PTMO, ST, DG, and CV. The Internet connection speed variable with indicators, normal connection, and the high connection was tested using a PLS-MGA analysis to assess the speed moderating effect between PTMO, ST, and DG and CV (see Table 20).

Table 20. PLS-MGA results for the internet connection speed moderating effect.

Exogenous Latent Variables	Normal Connection Speed		High Connection Speed		Normal vs. High		
	p(1)	se(*p(1)*)	*p(2)*	se(*p(2)*)	$\|p(1) - p(2)\|$	*t*-Value	*p*-Value
PTMO→CV	0.356	0.0653	0.496	0.0504	0.1404	0.761	0.447
ST→CV	0.158	0.0827	0.179	0.0595	0.0207	0.089	0.929
DG→CV	0.399	0.0620	0.239	0.0402	0.1595	0.912	0.362
N	672		85		-	-	-

PTMO = proximity to motivated offenders, ST = suitable target, DG = digital guardianship, CV = cyberstalking victimization.

The highest level of variance in path coefficient was observed in the relation between DG and CV (0.1595), with *t*-value = 0.912 and *p*-value = 0.362, which means that there was no statistical significance for the effect of Internet connection speed. Consequently, it was concluded that Internet connection speed is not a moderator between PTMO, ST, DG, and CV. The age variable was transformed to a categorical variable by combining the 16 indicators to become two indicators, which were: age $\leq$ 20 implies 18, 19 and 20 years old, and age > 20 implies 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 33, 38 and 42 (see the results in Table 21).

Table 21. PLS-MGA results for the age moderating effect.

Exogenous Latent Variables	Age > 20		Age $\leq$ 20		>20 vs. $\leq$20		
	p(1)	se(*p(1)*)	*p(2)*	se(*p(2)*)	$\|p(1) - p(2)\|$	*t*-Value	*p*-Value
PTMO→CV	0.338	0.0645	0.376	0.0637	0.0014	0.015	0.988
ST→CV	0.225	0.0881	0.067	0.0667	0.1579	1.310	0.190
DG→CV	0.306	0.0660	0.474	0.0535	0.1683	1.837	0.067
N	453		304		-	-	-

PTMO = proximity to motivated offenders, ST = suitable target, DG = digital guardianship, CV = cyberstalking victimization.

As shown in Table 21, the highest level of variance in path coefficient was observed in the relation between DG and CV (0.1683), with the *t*-value = 1.837* and *p*-value = 0.067, which indicated that there is a statistical significance for the effect of DG on the CV moderated by age. Consequently, it was concluded that age is a moderator with a significant effect between DG and CV. Other results did not exhibit any other significance. Place of residence was assessed as a categorical moderating effect using PLS-MGA since the frequencies and percentages for the five residence indicators were low compared with the indicator (city): 67.4%. This variable was assessed by dividing the data set into two subsets, which were city residence place and others, which included: desert (2.9%), refugee (8.6%), rural (3.3%), town (7.0%), and village (10.8%) (See the results in Table 22).

Table 22. PLS-MGA results for the place of residence moderating effect.

Exogenous Latent Variables	City		Others		City vs. Others		
	p(1)	se(*p(1)*)	*p(2)*	se(*p(2)*)	$\|p(1) - p(2)\|$	*t*-Value	*p*-Value
PTMO→CV	0.376	0.0647	0.328	0.0634	0.0483	0.470	0.639
ST→CV	0.097	0.0740	0.311	0.0913	0.2143	1.732	0.084
DG→CV	0.432	0.0615	0.288	0.0575	0.1442	1.488	0.137
N	510		247		-	-	-

PTMO = proximity to motivated offenders, ST = suitable target, DG = digital guardianship, CV = cyberstalking victimization.

As shown in Table 22, the highest level of variance in path coefficient was observed in the relation between ST and CV (0.2143), with *t*-value = 1.732* and *p*-value = 0.084, indicating that there is a statistical significance for the effect of ST on the CV moderated by residence. Consequently, it was concluded that the place of residence is a moderator between ST and CV. In the other results, no significance appeared. Based on the empir-

ical test, the confirmed conceptual model is based on assessing the structural model for cyberstalking victimization, as illustrated in Figure 8.

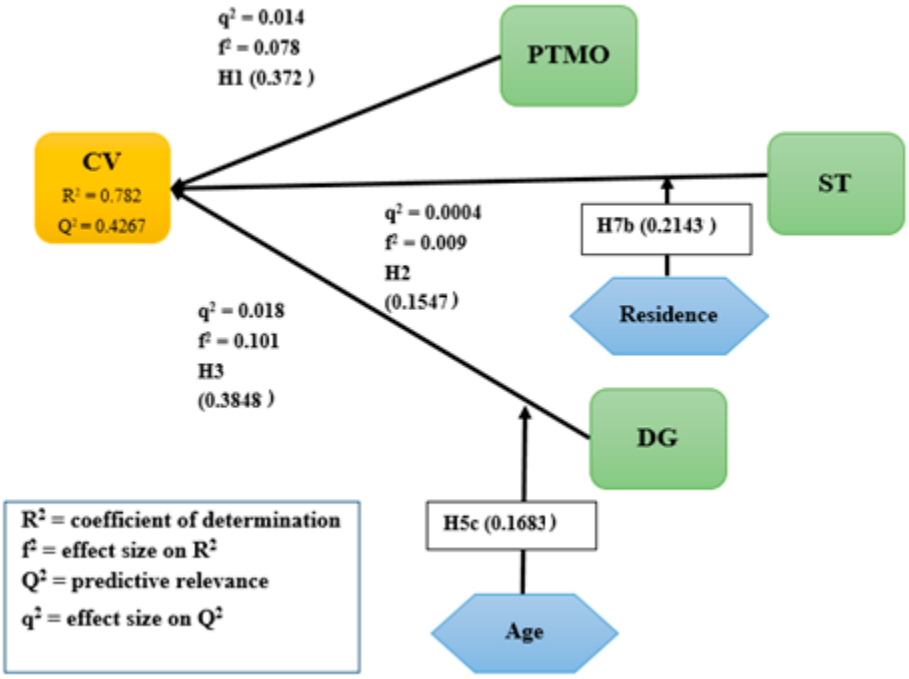

Figure 8. Confirmed structural model for cyberstalking victimization.

As can be seen in Figure 8, the coefficient of determination (R^2) for this model is 0.782, which means that the proximity of motivated offenders, a suitable target, and digital guardianship variables influence 78.2% of the variance in the cyberstalking victimization variable, which indicates a substantial range, indicating that these three variables can be explained or caused by 78.2% of the variance in the cyberstalking victimization variable. Since the R^2 value was between 0 to 1, and the higher the value, the better the fit, it is confirmed that the combined effects of these three exogenous variables were substantial and fitted the endogenous variable.

Concerning R^2 value, and moving on to test the effect size (f^2) of proximity to motivated offenders, a suitable target and digital guardianship on the dependent variable cyberstalking victimization, the results show that the proximity to motivated offenders variable had an impact with a small effect on cyberstalking victimization ($f^2 = 0.078$), the suitable target had an impact with a minimal effect ($f^2 = 0.009$) and digital guardianship also exhibited a minimal effect ($f^2 = 0.101$) on the cyberstalking victimization variable. These results indicated that the effects of the variables PTMO, ST, and DG on cyberstalking victimization have a substantial impact by combining, and there was no effect size for a particular variable separately on cyberstalking victimization, which means that the integration between the combined independent variables and the dependent variable was high and the model fits. The evaluation of the magnitude of the R^2 values as a criterion of predictive accuracy was done by using the predictive relevance (Q^2). The results show that the Q^2 value for this model is 0.4267, reflecting an excellent predictive relevance for cyberstalking victimization. This means that the proximity to motivated offenders, a suitable target, and digital guardianship constructs together predict the cyberstalking victimization construct. After that, the effect size of predictive relevance (q^2) was assessed; the results show that none of the independent constructs significantly affect the cyberstalking victimization construct. Proximity to motivated offenders, a suitable target, and digital guardianship show a small effect with values of 0.014, 0.0004, and 0.018, respectively, indicating that the confirmation of the integrated model constructs together shows an excellent predic-

tive relevance and better than predictive relevance for a single construct (0.4267 for the combination >0.014, 0.0004 and 0.018).

Hypotheses testing results exhibited five significant relationships. Although the significant relationships appeared in H1, H2, H3, H7b, and H5c, four of them were significant with the expected direction sign, and one of them was significant but with the other direction. For H1, the proximity to motivated offenders shows a significant positive effect on cyberstalking victimization (*t*-value = 5.8085 ***). The result matched the expectation that the more proximate/exposed to motivated offenders through lifestyle exposure online activities—chatting/instant messenger (text), chatting/instant messenger (voice), playing games, reading newspapers/magazines, sending/receiving emails, social networking sites, visiting religious websites, watching/downloading videos, listening to/downloading music and adding strangers on SNW/IM)—the greater the probability of experiencing cyberstalking victimization. It is not surprising that engaging in these online activities will frequently lead to becoming a victim of cyberstalking victimization.

The results were consistent with previous studies in terms of proximity/exposure to motivated offenders through online activities, and the variation of items could be the result of different methods of operationalization of the constructs. However, at least one item was consistent with the previous studies in the current study: for example, Marcum [159] found that increased exposure to motivated offenders has a sizable impact on the likelihood of victimization. Welsh and Lavoie [158] found that the frequency of 17 online activities was significantly associated with cyberstalking. Choi [217] found that engaging in online activities through risky activities (websites, downloading free games, music, and movies) and vocational and leisure activities (IM, shopping, watching newspapers) was positively significantly associated with victimization. Phillips [93] also found that risky activities through online SNS activity and risky leisure and vocational activities were positively associated with victimization. Reyns et al. [82] found that one item significantly related to victimization was online proximity, which allowed strangers to access personal online information about their victims. In addition, Back [77] found that active engagement in vocational and leisure activities on SNSs by adding unknown friends (strangers) significantly increased victimization. Holt and Bossler [156] found that spending more time on specific online activities (chatrooms, IRC/IM) increased the odds of being harassed, whereas Ngo and Paternoster [160] found that only IM was significant in terms of non-stranger harassment. Leukfeldt and Yar [162] investigated email, MSN, and Skype regarding online visibility and found that these forms of communication increased the risk of victimization. Yucedal [37] found that online leisure activities significantly affect victimization (spyware and Ad-Aware). Marcum et al. [161] and Bossler et al. [157] found a significant relationship between online activities and victimization. The former found that hours per week spent online (email, IM, SNW, and chatrooms) were significantly associated with victimization; the latter researcher found that the average hours per day spent online on social networking sites increased the odds of victimization. Thus, our findings reflected the findings of previous studies that engaging in online activities will increase the probability of experiencing online victimization, with variations in the results of different methods of operationalization of specific online activities that the researchers included in their studies.

Regarding H2, which was that a suitable target has a significant positive effect on cyberstalking victimization, the results show a conformation for this hypothesis (*t*-value = 1.9423 *). The results matched with the expectation that students who frequently exhibited their personal information, including age, email address, gender, name, photos, videos, bank account number, home address, mobile phone number, increased the attractiveness as victims, supported the expectation that the motivated offenders and their increased exposure made them a cyberstalking victim. The results showed a mixed reflection matching with the previous studies. The result findings are consistent with those of Marcum et al. [161], Reyns et al. [82], and Marcum [159]. In his study, Marcum [159] found that personal information posted on social networking sites and personal information given

to people online has a significant positive effect on victimization. Out of nine predictors, Reyns et al. [82] found that only two items were associated with online victimization, which was, firstly, that a student who showed his gender and relationship status frequently was associated significantly with cyberstalking victimization. Marcum et al. [161] also found in their results on exhibited personal information that communication with strangers, and types of personal information given to people, are significantly associated with online victimization.

In contrast to previous studies, in terms of significance [93,156,159,161,162], none found a significant effect between capable guardianship and online victimization. In contrast, Reyns et al. [82] found that one measure (online profile tracker), designed to monitor social network activities, had a significant relationship with cyberstalking victimization. In contrast to previous studies, in terms of direction [77,217], in his study, Choi [217] found that the number of computer security programs and duration were negatively significantly associated with victimization. Back [77] also found that the cyber security settings on SNSs and security applications reduced cyberharassment victimization. In line with previous studies, the test of the demographic variables shows mixed results. Five moderators tested the relationship between independent factors and cyberstalking victimization, and the results showed that H4, H5a, H5b, H6, H7a and H7c, and H8 were not whereas H5c and H7b were accepted.

H4 tests the moderating effect of gender between L-RAT factors (PTMO, SU, DG) and cyberstalking victimization. The *t*-value for the path coefficient differences shows 0.695, 1.002, and 0.459 for proximity to motivated offenders, a suitable target and digital guardianship, respectively (Ivs) on cyberstalking (Dv), indicating that there is no significant effect of gender between L-RAT factors and cyberstalking victimization, reflecting that gender is not a moderator for this model. The result is consistent with the previous studies of Ngo and Paternoster [160], Back [77], Yucedal [37] and Leukfeldt and Yar [162], and not with those of Reyns [36], Choi [217], Paullet [47], Alshalan [168] and Curtis [46]. The results of the previous studies depended on the operationalization of the constructs: for example, Paullet [47] found that gender was significant in reporting cyberstalking cases, and Curtis [46] found that gender plays a significant role in cyberstalking preparation.

H5 was tested, and the results show that age showed a moderate effect between digital guardianship and cyberstalking victimization (H5c) with a *t*-value = 1.837 *, with an insignificant effect for the other factors PTMO and SU (H5a and H5b). Therefore, it can be concluded that age is a moderator between digital guardianship and cyberstalking victimization. The result is consistent with the previous studies of Leukfeldt and Yar [162], Ngo and Paternoster [160], and Choi [217] and inconsistent with those of Holt and Bossler [156], Back [77], Yucedal [37], and Paullet [47]. Thus, H5 was accepted in terms of digital guardianship (H7c).

H6 and H8 concern Internet speed (average speed vs. high speed) and nationality (local vs. foreigner) as moderators between L-RAT factors and cyberstalking victimization. The results did not show any significant differences, so H6 and H8 were not accepted. Similiarly for H4, internet speed, and nationality were assumed as not moderators for the study's conceptual model. Although previous studies employed the frequency of Internet use and its effect on victimization, Holt, and Bossler [156] did not find any statistically significant effect between Internet speed and online victimization, consistent with the current study. H7 was tested, and the results show that place of residence (city vs. others) has a significant effect of the suitable target on cyberstalking victimization moderated by place of residence (*t*-value = 1.732 *), with an insignificant effect for others (PTMO, DG) on cyberstalking victimization. This indicates that H7 was accepted in terms of the suitable target (H7b).

8. Conclusions and Discussion

The main aim of this study was to investigate cyberstalking victimization among college students in Jordan. To achieve this objective, firstly, the prevalence of cyberstalking

victimization was estimated (objective 1). Secondly, the relationship between lifestyle routine activities theories and cyberstalking victimization constructs was examined (objective 2). Thirdly, the demographic variables associated with the experience of cyberstalking victimization were determined (objective 3). Finally, a conceptual model for cyberstalking victimization was developed and validated (objective 4).

To achieve the first objective of this study, which was to estimate the prevalence of cyberstalking victimization among college students, a systematic literature review was conducted using 14 online databases about the definition of cyberstalking. The definition was essential in order to operationalize the cyberstalking victimization construct through measures that will be used later to measure the cyberstalking victimization percentages through its types and lastly estimate the cyberstalking victimization and achieve this objective through 14 online databases, which were Science Direct, Scopus, Wiley Online Library, Springer, IEEE, ACM Digital Library, Emerald, Sage Journals, JSTOR, Cambridge Journals, Engineering, and Applied Science, ISI Web of Science, Oxford Journals, and Taylor and Francis Online, along with 46 extra materials. A total of 1179 materials were imported from Mendeley software after deleting duplicated materials. In phase II, NVivo data analysis software was used to organize and prepare the data for analysis by employing inclusion and exclusion criteria to choose the materials. Actual data coding was used in phase III to send the data about the prevalence of cyberstalking and create a cyberstalking prevalence node; then, among 24 materials that successfully matched the inclusion and exclusion criteria, the researcher filtered the measures operationalized the cyberstalking victimization construct. After that, the researcher adapted these measures to create the cyberstalking victimization constant. Next, the questionnaire was distributed to the local and overseas panel of experts as a validation procedure. Finally, by analyzing the results obtained from the respondents, the findings showed that the prevalence of cyberstalking victimization was between 39.92% and 66.76% depending on the cyberstalking behavior type. The findings showed a prevalence of 66.76%, 39.92%, 64.64%, 60.00%, 57.20%, 61.30%, 64.84%, and 49.18% for harassment and annoyance, posted false information, sent sexual material, pretended to be a victim, attempted to disable your computer, monitored your profile, sent the threatening letter or message to the victim's email, wrote threatening/offensive comments to the victim in chat rooms/instant messaging sites, respectively. The findings were consistent with previous studies and came within the range of 0.02% for Jerin and Dolinsky [218] to 82% for Bocij [18].

To address the second research objective of the study and examine the relationships between (L-RAT) and cyberstalking victimization, the same procedure for the first objective was carried out. A systematic literature review was conducted to extract the empirical studies for cyberstalking victimization, and only 12 studies matched the inclusion and exclusion criteria. The constructs under the (L-RAT) perspective with their measures were adapted to propose a conceptual model. As deductive research, this study identified a theoretical model to be a compass to examine the influencing factors and their relationships between L-RAT and cyberstalking victimization. After that, the model constructs and measures were given to the experts to validate them; then, model quality assessment was conducted by assessing the outer and inner models respectively using structural equation modeling (SEM) to validate the proposed model that has been created. Accordingly, and after refining the model, the hypotheses that were developed for testing the influencing factors of L-RAT) on cyberstalking victimization, and the examined relationships were tested. The results showed that all the factors for L-RAT (proximity to motivated offenders, suitable targets, and digital guardianship) had a significant positive relationship with cyberstalking victimization. The first two factors (PTMO, ST) were consistent with the expectation, whereas digital guardianship was contrary to the expectation.

To achieve the third objective of this study, which was to determine the demographic variables that are moderate and associated with the experience of cyberstalking victimization, five variables were proposed to have a moderating effect on the relations between the constructs and cyberstalking victimization. The results showed that gender, nationality,

and Internet connection speed did not significantly affect, whereas age showed a significant moderating effect between digital guardianship and cyberstalking victimization. The last moderator, who was a place of residence, showed a significant moderating effect between suitable target and cyberstalking victimization.

Finally, based on the detailed analysis for measurement and structural models, including hypotheses testing results that exhibited five significant relationships and after achieving the second and third objectives, the confirmed conceptual model for cyberstalking victimization was presented. Therefore, the fourth objective was achieved.

Several contributions have been made by achieving the objectives. The primary outcome of this study, which is a conceptual model for cyberstalking victimization, also has significant theoretical and practical implications. This research contributes to the body of knowledge by fulfilling the dire local (Jordan) need and developing the international perspective on cyberstalking victimization research. These contributions are:

i. Due to the following reasons, scientific evidence for the use of victimization and criminal opportunity explanations to account for cyberstalking victimization has been insufficient and contradictory to date:
    - The available studies on cyberstalking victimization have focused on the primary effect modeling without attention to any possible contextual effect.
    - The measurement used in the literature studies for the primary theoretical constructs (proximity/exposure to the motivated offender, a suitable target, and digital guardianship) may not have been appropriately operationalized, and depending on a single definition for the key theoretical concept [96], the current study operationalized the vital theoretical concepts systematically with their indicators depending on the systematic literature review on definitions and factors for cyberstalking victimization, which is assumed to be the first systematic literature review of cyberstalking victimization in the research.

This study contributes to the body of knowledge by expanding the importance of the L-RAT perspective for understanding victimization in the virtual world by testing the utility of L-RAT in cyberstalking victimization, which has been tested extensively in the traditional world. This study contributes to knowledge by shifting from the dominant focus on testing and studying stalking victimization to cyberstalking victimization. Based on the results, this study provides strong support for the applicability of the assumptions of L-RAT theory to cyberstalking victimization regarding PTMO and ST and partial support regarding digital guardianship. This study integrated routine activities theory and lifestyle exposure theory to become a power tester for cyberstalking victimization and other online victimization. The empirical investigation of the factors influencing cyberstalking victimization conduct keeping in view regarding the Jordan case.

8.1. Practical Implications

Cyberstalking is a relatively new phenomenon, and the scarce literature on this topic makes the investigation essentially an icebreaker in terms of the challenges, while assisting in giving a voice to the victims of cyberstalking. This study concluded that students who spend more time doing specific activities online would experience cyberstalking victimization. Further, students who appear to be suitable for targeting online by showing themselves to be attractive by exhibiting personal info will experience cyberstalking victimization. However, encouraging students to reduce their Internet usage is impossible, as Internet use is often necessary for many aspects of life. Therefore, it is fruitful to develop a model that can enhance awareness and improve cyberstalking victimization by determining the factors that influence it.

This study has developed and validated a conceptual model for cyberstalking victimization. It provides empirical evidence regarding what factors influence cyberstalking victimization, which can help the executive, legislative and judicial authorities, citizens, lawmakers, and others to make an accurate assessment of this phenomenon. This study has made two practical contributions:

i. A conceptual model for cyberstalking victimization that can be utilized to minimize the cyberstalking experienced by implementing it in society and providing research directions that will help us better understand the causes of this new phenomenon and what to do about it.
ii. This study has produced a validated questionnaire about cyberstalking victimization that can be used as an instrument tool by any institution in any society to uncover the prevalence and nature of the cyberstalking victimization phenomenon to contribute to its protective application. In conclusion, this study provides a comprehensive analysis of the factors and relationships that influence cyberstalking victimization and tests the moderator effect between these factors and cyberstalking victimization.

8.2. Limitations and Future Research Suggestions

Although the investigation supports the notion that cyberstalking is a problem among college students, as much research, the current study is not without its shortcomings. There are a few flaws in the analysis that will need to be fixed in subsequent studies.

The first drawback concerns conceptual analyses of cyberstalking and cyberharassment, which are difficult to compare owing to a lack of conceptual consistency and inconsistencies in word meanings. Therefore, a consistent concept of cyberstalking is required. Further analysis can be conducted using qualitative and quantitative approaches to understand further the phenomena and circumstances of cyberstalking and analyze the experiences of those subjected to these behaviors. The second drawback is the distinction between conventional and cyberstalking. Unfortunately, the current study did not look at the relationship between stalking and cyberstalking, so further analysis must figure out the differences and parallels. The third limitation is the research design for this study, which was cross-sectional. This introduced complications related to time ordering factors, on digital guardianship to resolve the time order issue, and future research should adopt a longitudinal design. The fourth limitation is related to the sample derived from a single student college in Jordan; this does not devalue our findings, but it is recommended that replication is necessary to represent other population units to improve the generalizability of the findings. The present analysis did not look at whether victims of bullying did not disclose the incidents; this fifth weakness should be addressed in future studies. Lastly, the current study was interested in one type of cybercrime, which was "cyberstalking." Future research is needed to assess the applicability of L-RAT to different types of cybercrime.

Author Contributions: W.A.-U.: conceptualization, supervision, methodology, formal analysis, resources, data curation, writing—original draft preparation. M.A.: conceptualization, supervision, writing—review and editing, project administration, funding acquisition. L.A.: conceptualization, writing–review and editing, supervision. A.A.A.: conceptualization, writing—review and editing, supervision. P.S.: conceptualization, writing—review and editing. A.H.G.: conceptualization, writing—review and editing. All authors have read and agreed to the published version of the manuscript.

Funding: This study was financially supported via a funding grant by Deanship of Scientific Research, Taif University Researchers Supporting Project number. TURSP-2020/300), Taif University, Taif, Saudi Arabia).

Acknowledgments: This study was financially supported via a funding grant by Deanship of Scientific Research, Taif University Researchers Supporting Project number. TURSP-2020/300, Taif University, Taif, Saudi Arabia.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Stats, I.W. World Internet Usage and Population Statistics 2021 Year-Q1 Estimates. Available online: https://www.internetworldstats.com/stats.htm (accessed on 31 March 2021).
2. Breslin, P. *An Investigation into the Problem of Cyberstalking in Ireland and an Examination of the Usefulness of Classifying Cyberstalking as an Addictive Disorder*; Dublin Business School: Dublin, Ireland, 2010.

3. Batra, S.; Sachdeva, S. Organizing Standardized Electronic Healthcare Records Data for Mining. *Health Policy Technol.* **2016**, *5*, 226–242. [CrossRef]
4. Broadhurst, R.; Grabosky, P.; Alazab, M.; Bouhours, B.; Chon, S. An analysis of the nature of groups engaged in cyber crime. *Int. J. Cyber Criminol.* **2014**, *8*, 1–20.
5. Chouhan, R. Cyber crimes: Evolution, detection and future challenges. *IUP J. Inf. Technol.* **2014**, *10*, 48.
6. Cox, C. Protecting victims of cyberstalking, cyberharassment, and online impersonation through prosecutions and effective laws. *Jurimetrics* **2014**, *54*, 277–302.
7. Harwood, M. *Security Strategies in Web Applications and Social Networking*; Jones & Bartlett Publishers: Burlington, MA, USA, 2010.
8. Hensler-McGinnis, N.F. *Cyberstalking Victimization: Impact and Coping Responses in a National University Sample*; University of Maryland: College Park, MD, USA, 2008.
9. Ladan, M.J. Overview of the 2015 Legal and Policy Strategy on Cybercrime and Cybersecurity in Nigeria. *SSRN Electron. J.* **2015**. [CrossRef]
10. Mahadevan, P. A Social Anthropology of Cybercrime, The Digitization of India's Economic Periphery. 2020. Available online: https://globalinitiative.net/analysis/cybercrime-india/ (accessed on 31 March 2021).
11. Schell, B.J. Internet Addiction and Cybercrime. In *The Palgrave Handbook of International Cybercrime and Cyberdeviance*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 679–703.
12. Seijen, S. *Risk Perception towards Cybercrime among Students in the Netherlands: The Effect of Multiple Factors on Risk Perception*; University of Twente: Enschede, The Netherlands, 2021.
13. Sissing, S.K. *A Criminological Exploration of Cyber Stalking in South Africa*; University of South Africa: Pretoria, South Africa, 2013.
14. Wall, D.S. *The Internet as a conduit for criminal activity. Information Technology and the Criminal Justice System*; Pattavina, A., Ed.; Sage Publications, Inc.: Newbury Park, CA, USA, 2015; pp. 77–98.
15. Johnson, L. *Computer Incident Response and Forensics Team Management: Conducting a Successful Incident Response*; Elsevier: Amsterdam, The Netherlands, 2013.
16. Basu, S. Jones, Law, and Technology. *Regul. Cyberstalking* **2007**, *2*, 1–30.
17. Bocij, P.; Griffiths, M.; McFarlane, L. Cyberstalking: A new challenge for criminal law. *Crim. Lawyer* **2002**, *122*, 3–5.
18. Bocij, P. Victims of cyberstalking: An exploratory study of harassment perpetrated via the Internet. *First Monday* **2002**, *8*. [CrossRef]
19. Dhillon, G.; Smith, K.J. Defining objectives for preventing cyberstalking. *J. Bus. Ethics* **2019**, *157*, 137–158. [CrossRef]
20. Dreßing, H. Cyberstalking in a large sample of social network users: Prevalence, characteristics, and impact upon victims. *Cyberpsychol. Behav. Soc. Netw.* **2014**, *17*, 61–67. [CrossRef]
21. Dreßing, H.; Klein, U.; Bailer, J.; Gass, P.; Gallas, C. Cyberstalking. *Nervenarzt* **2009**, *80*, 833–836. [CrossRef] [PubMed]
22. Easttom, C.; Taylor, J.; Hurley, H. *Computer Crime, Investigation, and the Law*; Course Technology: Boston, MA, USA, 2011.
23. Fukuchi, A. A balance of convenience: The use of burden-shifting devices in criminal cyberharassment law. *BCL Rev.* **2011**, *52*, 289.
24. Heinrich, P.A. *Generation iStalk: An Examination of the Prior Relationship between Victims of Stalking and Offenders*; Theses, Dissertations and Capstones; Marshall University: Huntington, WV, USA, 2015.
25. Henson, B. *Fear of Crime Online: Examining the Effects of Online Victimization and Perceived Risk on Fear of Cyberstalking Victimization*; University of Cincinnati: Cincinnati, OH, USA, 2011.
26. Henson, B.; Reyns, B.; Fisher, B. Internet crime. In *Key Issues in Crime and Punishment: Crime and Criminal Behavior*; Chambliss, W., Ed.; SAGE Publications: Thousand Oaks, CA, USA, 2011.
27. Leong, N.; Morando, J.J. Communication in cyberspace. *NCL Rev.* **2015**, *94*, 105.
28. Yang, Y.; Lutes, J.; Li, F.; Luo, B.; Liu, P. Stalking online: On user privacy in social networks. In Proceedings of the Second ACM Conference on Data and Application Security and Privacy, New York, NY, USA, 7–9 February 2012.
29. Lowry, P.B. Understanding and Predicting Cyberstalking in Social Media: Integrating Theoretical Perspectives on Shame, Neutralization, Self-Control, Rational Choice, and Social Learning. In Proceedings of the Journal of the Association for Information Systems Theory Development Workshop at the 2013 International Conference on Systems Sciences (ICIS 2013), Milan, Italy, 15–18 December 2013.
30. Maple, C.; Short, E.; Brown, A. *Cyberstalking in the United Kingdom: An Analysis of the ECHO Pilot Survey*; University of Bedfordshire: Luton, UK, 2011.
31. Mullen, P.E.; Pathé, M.; Purcell, R. *Stalkers and their Victims*; Cambridge University Press: Cambridge, UK, 2009.
32. Nobles, M.R.; Reyns, B.W.; Fox, K.A.; Fisher, B.S. Protection against pursuit: A conceptual and empirical comparison of cyberstalking and stalking victimization among a national sample. *Justice Q.* **2014**, *31*, 986–1014. [CrossRef]
33. Payne, B.K. Defining Cybercrime. In *The Palgrave Handbook of International Cybercrime and Cyberdeviance*; Springer: Cham, Switzerland, 2020; pp. 3–25.
34. Petrocelli, J.J.L.; Deerfield, O.-W.T. Cyberstalking Presenting a new challenge to law enforcement, cyberstalking occurs when electronic technology is utilized to create a criminal level of intimidation, harassment, or fear. *Law Order* **2005**, *53*, 56.
35. Spitzberg, B.H.; Hoobler, G. Cyberstalking and the technologies of interpersonal terrorism. *New Media Soc.* **2002**, *4*, 71–92. [CrossRef]

36. Reyns, B.W. *A* Situational crime prevention approach to cyberstalking victimization: Preventive tactics for Internet users and online place managers. *Crime Prev. Commun. Safety* **2010**, *12*, 99–118. [CrossRef]
37. Yucedal, B. *Victimization in Cyberspace: An Application of Routine Activity and Lifestyle Exposure Theories*; Kent State University: Kent, OH, USA, 2010.
38. Shorey, R.C.; Cornelius, T.L.; Strauss, C. Stalking in college student dating relationships: A descriptive investigation. *J. Fam. Violence* **2015**, *30*, 935–942. [CrossRef]
39. Elizondo, P.; McNiel, D.E.; Binder, R. A Review of Statutes and the Role of the Forensic Psychiatrist in Cyberstalking Involving Youth. *J. Am. Acad. Psychiatry Law* **2019**, *47*, 198–207.
40. Jaishankar, K.; Sankary, V. Cyber Stalking: A Global Menace in the Information Super Highway. *ERCES Online Q. Rev.* **2005**, *2*.
41. Kaplan, B. *Evaluating Health Care Information Systems: Methods and Applications*; SAGE Publications, Inc.: Newbury Park, CA, USA, 1994.
42. Kethineni, S. Cybercrime in India: Laws, Regulations, and Enforcement Mechanisms. In *The Palgrave Handbook of International Cybercrime and Cyberdeviance*; Springer: Cham, Switzerland, 2020; pp. 305–326.
43. Vasiu, I.; Vasiu, L. Cyberstalking Nature and response recommendations. *Acad. J. Interdiscip. Stud.* **2013**, *2*, 229. [CrossRef]
44. Reyns, B.W.; Henson, B.; Fisher, B. Stalking in the twilight zone: Extent of cyberstalking victimization and offending among college students. *Deviant Behav.* **2012**, *33*, 1–25. [CrossRef]
45. Cuenca-Piqueras, C.; Fernández-Prados, J.S.; González-Moreno, M.J. Face-to-face versus online harassment of European women: Importance of date and place of birth. *Sex. Cult.* **2020**, *24*, 157–173. [CrossRef]
46. Curtis, L.F. Virtual vs. Reality: An Examination of the Nature of Stalking and Cyberstalking; Citeseer: 2012. Available online: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.467.5711&rep=rep1&type=pdf (accessed on 31 March 2021).
47. Paullet, K.L. *An Exploratory Study of Cyberstalking: Students and Law Enforcement in Allegheny County, Pennsylvania*; Robert Morris University: Moon Twp, PA, USA, 2009.
48. Gialopsos, B.M.; Carter, J.W. Offender searches and crime events. *J. Contemp. Crim. Justice* **2015**, *31*, 53–70. [CrossRef]
49. Stansberry, K.; Anderson, J.; Rainie, L. Experts Optimistic About the Next 50 Years of Digital Life. 2019. Available online: https://www.newswise.com/articles/experts-optimistic-about-the-next-50-years-of-digital-life (accessed on 31 March 2021).
50. Gálik, S.; Galikova Tolnaiova, S. Cyberspace as a new existential dimension of man. In *Cyberspace*; Intech Open: London, UK, 2020; pp. 13–25.
51. Jahankhani, H.; Al-Nemrat, A.; Hosseinian-Far, A. Cybercrime classification and characteristics. In *Cyber Crime and Cyber Terrorism Investigator's Handbook*; Elsevier: Amsterdam, The Netherlands, 2014; pp. 149–164.
52. Tolnaiová, S.G.; Gálik, S. Cyberspace as a New Living World and Its Axiological Contexts. In *Cyberspace*; IntechOpen: London, UK, 2020.
53. Malby, S.; Jesrani, T.; Bañuelos, T.; Holterhof, A.; Hahn, M. *Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children*; United Nations Office on Drugs and Crime: Vienna, Austria, 2015.
54. Miller, J.J. Individual offending, routine activities, and activity settings: Revisiting the routine activity theory of general deviance. *J. Res. Crime Delinq.* **2013**, *50*, 390–416. [CrossRef]
55. Begotti, T.; Acquadro Maran, D. Characteristics of cyberstalking behavior, consequences, and coping strategies: A cross-sectional study in a sample of Italian university students. *Future Internet* **2019**, *11*, 120. [CrossRef]
56. Grunin, L.; Yu, G.; Cohen, S. The Relationship Between Youth Cyberbullying Behaviors and Their Perceptions of Parental Emotional Support. *Int. J. Bullying Prev.* **2020**. [CrossRef]
57. McLoughlin, L. Understanding and measuring coping with cyberbullying in adolescents: Exploratory factor analysis of the brief coping orientation to problems experienced inventory. *Curr. Psychol.* **2019**. [CrossRef]
58. Pittaro, M.L. Cyber stalking: An analysis of online harassment and intimidation. *Int. J. Cyber Criminol.* **2007**, *1*, 180–197.
59. Shimizu, A. Domestic violence in the digital age: Towards the creation of a comprehensive cyberstalking statute. *Berkeley J. Gend. Law Just.* **2013**, *28*, 116.
60. Gnasigamoney, S.S.; Sidhu, M.S. E-behaviour trends and patterns among Malaysian pre-adolescents and adolescents. *Int. J. Digit. Crime Forensics* **2013**, *5*, 50–62. [CrossRef]
61. Basu, S. Stalking the Stranger in Web 2.0: A Contemporary Regulatory Analysis. *Eur. J. Law Technol.* **2012**, *3*.
62. Meloy, J.R. Stalking: The State of the Science. *Crim. Behav. Ment. Health* **2007**, *17*, 1–7. [CrossRef]
63. Huffman, J.; Overton, A. Missing the Mark: The Neglect of Stalking and Cyberstalking in Introductory Criminology Textbooks. *J. Crim. Justice Educ.* **2013**, *24*, 200–217. [CrossRef]
64. Reyns, B.W. *Being Pursued Online: Extent and Nature of Cyberstalking Victimization from a Lifestyle/Routine Activities Perspective*; University of Cincinnati: Cincinnati, OH, USA, 2010.
65. Bossler, A.M.; Holt, D.J. On-line activities, guardianship, and malware infection: An examination of routine activities theory. *Int. J. Cyber Criminol.* **2009**, *3*, 400–420.
66. Holt, T.J.; Bossler, A.M. An Assessment of the Current State of Cybercrime Scholarship. *Deviant Behav.* **2014**, *35*, 20–40. [CrossRef]
67. Kirwan, G. *The Psychology of Cyber Crime: Concepts and Principles: Concepts and Principles*; IGI Global: Hershey, PA, USA, 2011.
68. Maple, C.; Wrixon, K. The Rise of Cyberstalking. In *Encyclopedia of Information Science and Technology*, 3rd ed.; IGI Global: Hershey, PA, USA, 2015; pp. 6801–6809.
69. Mishra, A.; Mishra, D. Cyber stalking: A challenge for web Security. *Cyber Warf. Cyber Terror.* **2007**, 216–226. [CrossRef]

70. Ogilvie, E. Cyberstalking. *Trends Issues Crime Crim. Justice* **2000**, *166*, 1–6.
71. Sheridan, L.P.; Grant, T. Is cyberstalking different? *Psychol. Crime Law* **2007**, *13*, 627–640. [CrossRef]
72. Van De Sandt, E. *Deviant Security: The Technical Computer Security Practices of Cyber Criminals*; University of Bristol: Bristol, UK, 2019.
73. Alshuaibi, A.S.; Mohd Shamsudin, F.; Alshuaibi, M.S.I. Internet misuse at work in Jordan: Challenges and implications. In Proceedings of the 3rd Convention of the World Association of Business Schools (WAiBS), Kuala Lumpur, Malaysia, 22 November 2015.
74. (TRC), J.T.R.C. Annual Report of 2015. 2015. Available online: https://www.cbsl.gov.lk/en/publications/economic-and-financial-reports/annual-reports/annual-report-2015 (accessed on 31 March 2021).
75. Faqir, R.S. Cyber Crimes in Jordan: A Legal Assessment on the Effectiveness of Information System Crimes Law No (30) of 2010. *Int. J. Cyber Criminol.* **2013**, *7*, 81–90.
76. Piotrowski, C.; Lathrop, P.J. Cyberstalking and college-age students: A bibliometric analysis across scholarly databases. *Coll. Stud. J.* **2012**, *46*, 533–536.
77. Back, S. Empirical Assessment of Cyber Harassment Victimization via Cyber-Routine Activities Theory. Master's Theses, Ball State University, Muncie, IN, USA, 2016.
78. DeTardo-Bora, K.A.; Bora, D.J. Cybercrimes: An overview of contemporary challenges and impending threats. *Digit. Forensics* **2016**, 119–132. [CrossRef]
79. Reyns, B.W. A routine activity perspective on online victimisation: Results from the Canadian General Social Survey. *J. Financ. Crime* **2015**. [CrossRef]
80. Finn, J. A Survey of Online Harassment at a University Campus. *J. Interpers. Violence* **2004**, *19*, 468–483. [CrossRef]
81. Parsons-Pollard, N.; Moriarty, L.J. Cyberstalking: Utilizing what we do know. *Vict. Offenders* **2009**, *4*, 435–441. [CrossRef]
82. Reyns, B.W.; Henson, B.; Fisher, B.S. Being pursued online: Applying cyberlifestyle–routine activities theory to cyberstalking victimization. *Crim. Justice Behav.* **2011**, *38*, 1149–1169. [CrossRef]
83. Reyns, B.W.; Henson, B. The thief with a thousand faces and the victim with none: Identifying determinants for online identity theft victimization with routine activity theory. *Int. J. offender Ther. Comp. Criminol.* **2016**, *60*, 1119–1139. [CrossRef]
84. Roberts, L. Jurisdictional and definitional concerns with computer-mediated Interpersonal crimes: An Analysis on Cyber Stalking. *Int. J. Cyber Criminol.* **2008**, *2*, 271–285.
85. Henson, B.; Reyns, B.W.; Fisher, B.S. Does gender matter in the virtual world? Examining the effect of gender on the link between online social network activity, security and interpersonal victimization. *Secur. J.* **2013**, *26*, 315–330. [CrossRef]
86. Henson, B.; Reyns, B.W.; Fisher, B.S. Cybercrime victimization. In *The Wiley Handbook on the Psychology of Violence*; Wily: Hoboken, NJ, USA, 2016; pp. 553–570. [CrossRef]
87. Moriarty, L.J.; Freiberger, K. Cyberstalking: Utilizing newspaper accounts to establish victimization patterns. *Vict. Offenders* **2008**, *3*, 131–141. [CrossRef]
88. Reyns, B.W.; Henson, B.; Fisher, B.S. Guardians of the cyber galaxy: An empirical and theoretical analysis of the guardianship concept from routine activity theory as it applies to online forms of victimization. *J. Contemp. Crim. Justice* **2016**, *32*, 148–168. [CrossRef]
89. Methe, T.D.; Meier, R.F. Opportunity, Choice, and Criminal Victimization: A Test of a Theoretical Model. *J. Res. Crime Delinq.* **1990**, *27*, 243–266. [CrossRef]
90. Cohen, L.E.; Felson, M. Social Change and Crime Rate Trends: A Routine Activity Approach. *Am. Sociol. Rev.* **1979**, *44*, 588. [CrossRef]
91. Hindelang, M.J.; Gottfredson, M.R.; Garofalo, J. *Victims of Personal Crime: An Empirical Foundation for a Theory of Personal Victimization*; Ballinger: Cambridge, MA, USA, 1978.
92. Cohen, L.E.; Kluegel, J.R.; Land, K.C. Social Inequality and Predatory Criminal Victimization: An Exposition and Test of a Formal Theory. *Am. Sociol. Rev.* **1981**, *46*, 505. [CrossRef]
93. Phillips, E. Empirical Assessment of Lifestyle-Routine Activity and Social Learning Theory on Cybercrime Offending. Master's Theses, Ball State University, Muncie, IN, USA, 2015.
94. Choi, K.S. Computer crime victimization and integrated theory: An empirical assessment. *Int. J. Cyber Criminol.* **2008**, *2*, 308–333.
95. Miethe, T.D.; Stafford, M.C.; Sloane, D. Lifestyle changes and risks of criminal victimization. *J. Quant. Criminol.* **1990**, *6*, 357–376. [CrossRef]
96. Vakhitova, Z.I.; Reynald, D.; Townsley, M. Toward the Adaptation of Routine Activity and Lifestyle Exposure Theories to Account for Cyber Abuse Victimization. *J. Contemp. Crim. Justice* **2016**, *32*, 169–188. [CrossRef]
97. FELSON, M. Linking Criminal Choices, Routine Activities, Informal Control, and Criminal Outcomes (1986). In *Classics in Environmental Criminology*; Routledge: London, UK, 2010; pp. 357–366.
98. Safaldin, M.; Otair, M.; Abualigah, L. Improved binary gray wolf optimizer and SVM for intrusion detection system in wireless sensor networks. *J. Ambient Intell. Hum. Comp.* **2021**, *12*, 1559–1576. [CrossRef]
99. McNeeley, S. Lifestyle-Routine Activities and Crime Events. *J. Contemp. Crim. Justice* **2015**, *31*, 30–52. [CrossRef]
100. Fnkelhor, D.; Asdigian, N.L. Risk factors for youth victimization: Beyond a lifestyles/routine activities theory approach. *Violence Vict.* **1996**, *11*, 3–20. [CrossRef]
101. Felson, M.; Clarke, R.V. Opportunity makes the thief. *Police Res. Ser. Pap.* **1998**, *98*, 10.

102. Abualigah, L.; Diabat, A.; Abd Elaziz, M. Intelligent workflow scheduling for Big Data applications in IoT cloud computing environments. In *Cluster Computing*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 1–20.
103. Clarke, R.V.G.; Webb, B. *Hot Products: Understanding, Anticipating and Reducing Demand for Stolen Goods*; Great Britain Home Office: London, UK, 1999.
104. Clarke, R.V.; Eck, J.E. *Crime Analysis for Problem Solvers in 60 Small Steps*; US Department of Justice, Office of Community Oriented Policing Services: Washington, DC, USA, 2005.
105. Miethe, T.D.; Meier, R.F. *Crime and Its Social Context: Toward an Integrated Theory of Offenders, Victims, and Situations*; Suny Press: New York, NY, USA, 1994.
106. Fisher, B. *The Sexual Victimization of College Women*; US Department of Justice, Office of Justice Programs, National Institute of Justice: Washington, DC, USA, 2000.
107. Tewksbury, R.; Mustaine, E.E. Routine Activities And Vandalism: A Theoretical And Empirical Study. *J. Crime Justice* **2000**, *23*, 81–110. [CrossRef]
108. Chen, L.E.; Cantor, D. Residential Burglary in the United States: Life-Style and Demographic Factors Associated With the Probability of Victimization. *J. Res. Crime Delinq.* **1981**, *18*, 113–127. [CrossRef]
109. Jensen, G.F.; Brownfield, D. Gender, Lifestyles, and Victimization: Beyond Routine Activity. *Violence Vict.* **1986**, *1*, 85–99. [CrossRef]
110. Methe, T.D.; Stafford, M.C.; Long, J.S. Social Differentiation in Criminal Victimization: A Test of Routine Activities/Lifestyle Theories. *Am. Sociol. Rev.* **1987**, *52*, 184. [CrossRef]
111. Sampson, R.J. Personal Violence by Strangers: An Extension and Test of the Opportunity Model of Predatory Victimization. *J. Crim. Law Criminol.* **1987**, *78*, 327. [CrossRef]
112. Sampson, R.J.; Wooldredge, J.D. Linking the micro-and macro-level dimensions of lifestyle-routine activity and opportunity models of predatory victimization. *J. Quant. Criminol.* **1987**, *3*, 371–393. [CrossRef]
113. Lasley, J.R. Drinking routines/lifestyles and predatory victimization: A causal analysis. *Justice Q.* **1989**, *6*, 529–542. [CrossRef]
114. Kennedy, L.W.; Forde, D.R. Routine Activities and Crime: An Analysis of Victimization in Canada. *Criminology* **1990**, *28*, 137–152. [CrossRef]
115. Sampson, R.J.; Lauritsen, J.L. Deviant Lifestyles, Proximity to Crime, and the Offender-Victim Link in Personal Violence. *J. Res. Crime Delinq.* **1990**, *27*, 110–139. [CrossRef]
116. Luritsen, J.L.; Sampson, R.J.; Laub, J.H. The link between offending and victimization among adolescents. *Criminology* **1991**, *29*, 265–292. [CrossRef]
117. Lauritsen, J.L.; Laub, J.H.; Sampson, R.J. Conventional and Delinquent Activities: Implications for the Prevention of Violent Victimization among Adolescents. *Violence Vict.* **1992**, *7*, 91–108. [CrossRef] [PubMed]
118. Wooldredge, J.D.; Cullen, F.T.; Latessa, E.J. Research note victimization in the workplace: A test of routine activities theory. *Justice Q.* **1992**, *9*, 325–335. [CrossRef]
119. Miethe, T.D.; McDowall, D.J. Contextual effects in models of criminal victimization. *Soc. Forces* **1993**, *71*, 741–759. [CrossRef]
120. Rountree, P.W.; Land, K.C.; Miethe, T.D. Macro-micro integration in the study of victimization: A hierarchical logistic model analysis across seattle neighborhoods. *Criminology* **1994**, *32*, 387–414. [CrossRef]
121. Schwartz, M.D.; Pitts, V.L. Exploring a feminist routine activities approach to explaining sexual assault. *Justice Q.* **1995**, *12*, 9–31. [CrossRef]
122. Fisher, B.S.; Sloan, J.; Cullen, F.T.; Lu, C. Crime in the ivory tower: The level and sources of student victimization. *Criminology* **1998**, *36*, 671–710. [CrossRef]
123. Mustaine, E.E.; Tewksbury, R. Predicting Risks of Larceny theft victimization: A routine activity analysis using refined lifestyle measures. *Criminology* **1998**, *36*, 829–858. [CrossRef]
124. Mustaine, E.E.; Tewksbury, R.J. A routine activity theory explanation for women's stalking victimizations. *Violence Women* **1999**, *5*, 43–62. [CrossRef]
125. Mustaine, E.E.; Tewksbury, R. Comparing the Lifestyles of Victims, Offenders, and Victim-Offenders: A Routine Activity Theory Assessment of Similarities and Differences for Criminal Incident Participants. *Sociol. Focus* **2000**, *33*, 339–362. [CrossRef]
126. Wittebrood, K.; Nieuwbeerta, P. Criminal victimization during one's life course: The effects of previous victimization and patterns of routine activities. *J. Res. Crime Delinq.* **2000**, *37*, 91–122. [CrossRef]
127. Fisher, B.S.; Cullen, F.T.; Turner, M.G. Being pursued: Stalking victimization in a national study of college women. *Criminol. Publ. Policy* **2002**, *1*, 257–308. [CrossRef]
128. Mustaine, E.E.; Tewksbury, R. Sexual Assault of College Women: A Feminist Interpretation of a Routine Activities Analysis. *Crim. Justice Rev.* **2002**, *27*, 89–123. [CrossRef]
129. Schreck, C.; Wright, R.A.; Miller, J.M. A study of individual and situational antecedents of violent victimization. *Justice Q.* **2002**, *19*, 159–180. [CrossRef]
130. Dugan, L.; Apel, R. An exploratory study of the violent victimization of women: Race/Ethnicity and situational context. *Criminology* **2003**, *41*, 959–980. [CrossRef]
131. Schreck, C.; Miller, J.M.; Gibson, C.L. Trouble in the School Yard: A Study of the Risk Factors of Victimization at School. *Crime Delinq.* **2003**, *49*, 460–484. [CrossRef]

132. Schreck, C.J.; Fisher, B.S. Specifying the influence of family and peers on violent victimization: Extending routine activities and lifestyles theories. *J. Interpers. Violence* **2004**, *19*, 1021–1041. [CrossRef] [PubMed]
133. Tseloni, A.; Wittebrood, K.; Farrell, G.; Pease, K. Burglary Victimization in England and Wales, the United States and the Netherlands: A Cross-National Comparative Test of Routine Activities and Lifestyle Theories. *Br. J. Criminol.* **2004**, *44*, 66–91. [CrossRef]
134. Schreck, C.J.; Stewart, E.A.; Fisher, B.S. Self-control, Victimization, and their Influence on Risky Lifestyles: A Longitudinal Analysis Using Panel Data. *J. Quant. Criminol.* **2006**, *22*, 319–340. [CrossRef]
135. Wilcox, P.; Madensen, T.D.; Tillyer, M.S. Guardianship in Context: Implications for burglary victimization risk and prevention. *Criminology* **2007**, *45*, 771–803. [CrossRef]
136. Messner, S.F.; Lu, Z.; Zhang, L.; Liu, J. Risks of Criminal Victimization in Contemporary Urban China: An Application of Lifestyle/Routine Activities Theory. *Justice Q.* **2007**, *24*, 496–522. [CrossRef]
137. Taylor, T.J.; Peterson, D.; Esbensen, F.-A.; Freng, A. Gang Membership as a Risk Factor for Adolescent Violent Victimization. *J. Res. Crime Delinq.* **2007**, *44*, 351–380. [CrossRef]
138. Taylor, T.J. Youth gang membership and serious violent victimization: The importance of lifestyles and routine activities. *J. Interpers. Violence* **2008**, *23*, 1441–1464. [CrossRef]
139. Spano, R.; Freilich, J.D.; Bolland, J. Gang Membership, Gun Carrying, and Employment: Applying Routine Activities Theory to Explain Violent Victimization Among Inner City, Minority Youth Living in Extreme Poverty*. *Justice Q.* **2008**, *25*, 381–410. [CrossRef]
140. Burrow, J.D.; Apel, R. Youth Behavior, School Structure, and Student Risk of Victimization. *Justice Q.* **2008**, *25*, 349–380. [CrossRef]
141. Wilcox, P. Gendered opportunity? School-based adolescent victimization. *J. Res. Crime Delinq.* **2009**, *46*, 245–269. [CrossRef]
142. Savolainen, J.; Sipilä, P.; Martikainen, P.; Anderson, A.L. Family, Community, and Lifestyle: Adolescent Victimization in Helsinki. *Sociol. Q.* **2009**, *50*, 715–738. [CrossRef]
143. Reid, J.A.; Sullivan, C.J. A Latent Class Typology of Juvenile Victims and Exploration of Risk Factors and Outcomes of Victimization. *Crim. Justice Behav.* **2009**, *36*, 1001–1024. [CrossRef]
144. Henson, B.; Wilcox, P.; Reyns, B.W.; Cullen, F.T. Gender, Adolescent Lifestyles, and Violent Victimization: Implications for Routine Activity Theory. *Vict. Offenders* **2010**, *5*, 303–328. [CrossRef]
145. Fisher, B.S.; Daigle, L.E.; Cullen, F.T. What Distinguishes Single from Recurrent Sexual Victims? The Role of Lifestyle-Routine Activities and First-Incident Characteristics. *Justice Q.* **2010**, *27*, 102–129. [CrossRef]
146. Tillyer, M.S.; Wilcox, P.; Gialopsos, B.M. Adolescent school-based sexual victimization: Exploring the role of opportunity in a gender-specific multilevel analysis. *J. Crim. Justice* **2010**, *38*, 1071–1081. [CrossRef]
147. Sillyer, M.S.; Tillyer, R.; Miller, H.V.; Pangrac, R. Reexamining the Correlates of Adolescent Violent Victimization: The Importance of Exposure, Guardianship, and Target Characteristics. *J. Interpers. Violence* **2010**, *26*, 2908–2928. [CrossRef]
148. Tillyer, M.S.; Fisher, B.S.; Wilcox, P.J. The effects of school crime prevention on students' violent victimization, risk perception, and fear of crime: A multilevel opportunity perspective. *Justice Q.* **2011**, *28*, 249–277. [CrossRef]
149. Peguero, A.A.; Popp, A.M.; Koo, D.J. Race, Ethnicity, and School-Based Adolescent Victimization. *Crime Delinq.* **2015**, *61*, 323–349. [CrossRef]
150. Pauwels, L.J.R.; Svensson, R. Exploring the Relationship Between Offending and Victimization: What is the Role of Risky Lifestyles and Low Self-Control? A Test in Two Urban Samples. *Eur. J. Crim. Policy Res.* **2011**, *17*, 163–177. [CrossRef]
151. Averdijk, M. Reciprocal Effects of Victimization and Routine Activities. *J. Quant. Criminol.* **2011**, *27*, 125–149. [CrossRef]
152. Peguero, A.A.; Popp, A.M. Youth violence at school and the intersection of gender, race, and ethnicity. *J. Crim. Justice* **2012**, *40*, 1–9. [CrossRef]
153. Maimon, D.; Browning, C.R. Adolescents' Violent Victimization in the Neighbourhood: Situational and Contextual Determinants. *Br. J. Criminol.* **2012**, *52*, 808–833. [CrossRef]
154. Bunch, J.; Clay-Warner, J.; Lei, M.K. Demographic characteristics and victimization risk: Testing the mediating effects of routine activities. *Crime Delinq.* **2015**, *61*, 1181–1205. [CrossRef]
155. Gibson, C.L.; Fagan, A.A.; Antle, K. Avoiding Violent Victimization Among Youths in Urban Neighborhoods: The Importance of Street Efficacy. *Am. J. Public Health* **2014**, *104*, e154–e161. [CrossRef] [PubMed]
156. Holt, T.J.; Bossler, A.M. Examining the Applicability of Lifestyle-Routine Activities Theory for Cybercrime Victimization. *Deviant Behav.* **2008**, *30*, 1–25. [CrossRef]
157. Bossler, A.M.; Holt, T.J.; May, D.C. Predicting Online Harassment Victimization Among a Juvenile Population. *Youth Soc.* **2012**, *44*, 500–523. [CrossRef]
158. Welsh, A.; Lavoie, J.A.A. Risky eBusiness: An Examination of Risk-taking, Online Disclosiveness, and Cyberstalking Victimization. *Cyberpsychol. J. Psychosoc. Res. Cyberspace* **2012**, *6*. [CrossRef]
159. Marcum, C.D. Identifying potential factors of adolescent online victimization for high school seniors. *Int. J. Cyber Criminol.* **2008**, *2*, 346.
160. Ngo, F.T.; Paternoster, R. Cybercrime Victimization: An examination of Individual and Situational level factors. *Int. J. Cyber Criminol.* **2011**, *5*, 773.
161. Marcum, C.D.; Ricketts, M.L.; Higgins, G.E. Assessing sex experiences of online victimization: An examination of adolescent online behaviors using routine activity theory. *Crim. Justice Rev.* **2010**, *35*, 412–437. [CrossRef]

162. Leukfeldt, E.R.; Yar, M. Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis. *Deviant Behav.* **2016**, *37*, 263–280. [CrossRef]
163. Hutchings, A.; Hayes, H. Routine activity theory and phishing victimisation: Who gets caught in the 'net'? *Curr. Issues Crim. Justice* **2009**, *20*, 433–452. [CrossRef]
164. Pratt, T.C.; Holtfreter, K.; Reisig, M.D. Routine Online Activity and Internet Fraud Targeting: Extending the Generality of Routine Activity Theory. *J. Res. Crime Delinq.* **2010**, *47*, 267–296. [CrossRef]
165. Van Wilsem, J. Worlds tied together? Online and non-domestic routine activities and their impact on digital and traditional threat victimization. *Eur. J. Criminol.* **2011**, *8*, 115–127. [CrossRef]
166. Leukfeldt, E.R. Phishing for suitable targets in the Netherlands: Routine activity theory and phishing victimization. *Cyberpsychol. Behav. Soc. Netw.* **2014**, *17*, 551–555. [CrossRef] [PubMed]
167. Van Wilsem, J. 'Bought it, but Never Got it' Assessing Risk Factors for Online Consumer Fraud Victimization. *Eur. Sociol. Rev.* **2013**, *29*, 168–178. [CrossRef]
168. Alshalan, A. *Cyber-Crime Fear and Victimization: An Analysis of a National Survey*; Mississippi State University: Starkville, MS, USA, 2006.
169. Navarro, J.N.; Jasinski, J. Going Cyber: Using Routine Activities Theory to Predict Cyberbullying Experiences. *Sociol. Spectr.* **2012**, *32*, 81–94. [CrossRef]
170. Marcum, C.D.; Higgins, G.E.; Ricketts, M.L. Potential Factors of Online Victimization of Youth: An Examination of Adolescent Online Behaviors Utilizing Routine Activity Theory. *Deviant Behav.* **2010**, *31*, 381–410. [CrossRef]
171. Reyns, B.W. Online routines and identity theft victimization: Further expanding routine activity theory beyond direct-contact offenses. *J. Res. Crime Delinq.* **2013**, *50*, 216–238. [CrossRef]
172. Wiersma, W. *Research Methods in Education: An Introduction*; Prentice Hall: Upper Saddle River, NJ, USA, 1985.
173. Guba, E.G.; Lincoln, Y.S. Competing paradigms in qualitative research. *Handb. Qual. Res.* **1994**, *2*, 105.
174. Bamasoud, D.M.; Iahad, N.A.; Rahman, A.A. Academic researchers' absorptive capacity influence on collaborative technologies acceptance for research purpose: Pilot study. *Mod. Appl. Sci.* **2014**, *8*, 161. [CrossRef]
175. Bhattacherjee, A. *Social Science Research: Principles, Methods, and Practices*; Global Text Project: Athens, GA, USA, 2012.
176. Kennedy, M.A.; Taylor, M.A. Online harassment and victimization of college students. *Justice Policy J.* **2010**, *7*, 1–21.
177. Sekaran, U.; Bougie, R. *Research Methods for Business: A Skill Building Approach*; John Wiley & Sons: Hoboken, NJ, USA, 2016.
178. Blaxter, L. *How to Research*; McGraw-Hill Education: New York, NY, USA, 2010.
179. Hair Jr, J.F.; Hult, G.T.M.; Ringle, C.; Sarstedt, M. *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*; Sage Publications: Thousand Oaks, CA, USA, 2016.
180. Edwards, J.R.; Bagozzi, R.P. On the nature and direction of relationships between constructs and measures. *Psychol. Methods* **2000**, *5*, 155–174. [CrossRef]
181. Maccallum, R.C.; Browne, M.W. The use of causal indicators in covariance structure models: Some practical issues. *Psychol. Bull.* **1993**, *114*, 533–541. [CrossRef] [PubMed]
182. Petter, S.; Straub, D.; Rai, A. Specifying Formative Constructs in Information Systems Research. *MIS Q.* **2007**, *31*, 623. [CrossRef]
183. Diamantopoulos, A.; Winklhofer, H.M. Index construction with formative indicators: An alternative to scale development. *J. Mark. Res.* **2001**, *38*, 269–277. [CrossRef]
184. Fornell, C.; Bookstein, F.L. Two structural equation models: LISREL and PLS applied to consumer exit-voice theory. *J. Mark. Res.* **1982**, *19*, 440–452. [CrossRef]
185. Rossiter, J.R. The C-OAR-SE procedure for scale development in marketing. *Int. J. Res. Mark.* **2002**, *19*, 305–335. [CrossRef]
186. Chin, W.W. The partial least squares approach to structural equation modeling. *Mod. Methods Bus. Res.* **1998**, *295*, 295–336.
187. Jarvis, C.B.; MacKenzie, S.B.; Podsakoff, P.M. A Critical Review of Construct Indicators and Measurement Model Misspecification in Marketing and Consumer Research. *J. Consum. Res.* **2003**, *30*, 199–218. [CrossRef]
188. Cronbach, L.J. Coefficient alpha and the internal structure of tests. *Psychometrika* **1951**, *16*, 297–334. [CrossRef]
189. Gefen, D.; Straub, D.; Boudreau, M.C. Structural equation modeling and regression: Guidelines for research practice. *Commun. Assoc. Inf. Syst.* **2000**, *4*, 7. [CrossRef]
190. Urbach, N.; Ahlemann, F. Structural equation modeling in information systems research using partial least squares. *J. Inf. Technol. Theory Appl.* **2010**, *11*, 5–40.
191. Hair, J. *Multivariate Data Analysis Seventh Edition*; Prentice Hall: Upper Saddle River, NJ, USA, 2010.
192. Kasunic, M. *Designing an Effective Survey*; Carnegie-Mellon Univ Pittsburgh PA Software Engineering Inst: Pittsburgh, PA, USA, 2005.
193. Netemeyer, R.G.; Bearden, W.O.; Sharma, S. *Scaling Procedures: Issues and Applications*; Sage Publications: Thousand Oaks, CA, USA, 2003.
194. Zukerberg, A.L.; Moore, J.C.; Von Thurn, D.R. *Practical Considerations in Sample Size Selection for Behavior Coding Pretests*; US Bureau of the Census: Washington, DC, USA, 1995.
195. Harter, R.; Eckman, S.; English, N.; O'Muircheartaigh, C. Applied sampling for large-scale multi-stage area probability designs. *Handb. Surv. Res.* **2010**, *2*, 169–199.
196. Sim, J.; Lewis, M. The size of a pilot study for a clinical trial should be calculated in relation to considerations of precision and efficiency. *J. Clin. Epidemiol.* **2012**, *65*, 301–308. [CrossRef] [PubMed]

197. Cooper, D.R.; Schindler, P.S.; Sun, J. *Business Research Methods*; Mcgraw-Hill: New York, NY, USA, 2006; Volume 9.
198. Thabane, L.; Ma, J.; Chu, R.; Cheng, J.; Ismaila, A.; Rios, L.P.; Robson, R.; Thabane, M.; Giangregorio, L.; Goldsmith, C.H. A tutorial on pilot studies: The what, why and how. *BMC Med Res. Methodol.* **2010**, *10*, 1. [CrossRef] [PubMed]
199. Garofalo, J. *Reassessing the Lifestyle Model of Criminal Victimization*; Sage Publications: Thousand Oaks, CA, USA, 1987; pp. 23–42.
200. Straub, D.; Boudreau, M.C.; Gefen, D. Validation guidelines for IS positivist research. *Commun. Assoc. Inf. Syst.* **2004**, *13*, 24. [CrossRef]
201. Lewis, B.R.; Templeton, G.F.; Byrd, T.A. A methodology for construct development in MIS research. *Eur. J. Inf. Syst.* **2005**, *14*, 388–400. [CrossRef]
202. Anderson, J.C.; Gerbing, D.W. Structural equation modeling in practice: A review and recommended two-step approach. *Psychol. Bull.* **1988**, *103*, 411. [CrossRef]
203. Bagozzi, R.P.; Yi, Y.; Phillips, L.W. Assessing Construct Validity in Organizational Research. *Adm. Sci. Q.* **1991**, *36*, 421. [CrossRef]
204. Chin, W.W. How to write up and report PLS analyses. In *Handbook of Partial Least Squares*; Springer: Cham, Switzerland, 2010; pp. 655–690.
205. Campbell, D.T.; Fiske, D.W. Convergent and discriminant validation by the multitrait-multimethod matrix. *Psychol. Bull.* **1959**, *56*, 81. [CrossRef]
206. Fornell, C.; Larcker, D.F. Evaluating structural equation models with unobservable variables and measurement error. *J. Mark. Res.* **1981**, *18*, 39–50. [CrossRef]
207. Henseler, J.; Ringle, C.M.; Sinkovics, R.R. The use of partial least squares path modeling in international marketing. In *New Challenges to International Marketing*; Emerald Group Publishing Limited: Bingley, UK, 2009.
208. Geisser, S.; Eddy, W.F. A predictive approach to model selection. *J. Am. Stat. Assoc.* **1979**, *74*, 153–160. [CrossRef]
209. Stone, M. Cross-Validatory Choice and Assessment of Statistical Predictions. *J. R. Stat. Soc. Ser. B Stat. Methodol.* **1974**, *36*, 111–133. [CrossRef]
210. Abualigah, L.M.Q. *Feature Selection and Enhanced Krill Herd Algorithm for Text Document Clustering*; Springer: Cham, Switzerland, 2019.
211. Abualigah, L.; Diabat, A.; Mirjalili, S.; Elaziz, M.A.; Gandomi, A.H. The Arithmetic Optimization Algorithm. *Comput. Methods Appl. Mech. Eng.* **2021**, *376*, 113609. [CrossRef]
212. Şahin, C.B.; Dinler, Ö.B.; Abualigah, L. Prediction of Software Vulnerability Based Deep Symbiotic Genetic Algorithms: Phenotyping of Dominant-Features. *Appl. Intell.* **2021**. [CrossRef]
213. Şahin, C.B.; Abualigah, L. A novel deep learning-based feature selection model for improving the static analysis of vulnerability detection. *Neural Comput. Appl.* **2021**. [CrossRef]
214. Abualigah, L.; Yousri, D.; Abd Elaziz, M.; Ewees, A.A.; Al-qaness, M.A.; Gandomi, A.H. Aquila Optimizer: A Novel Meta-Heuristic Optimization Algorithm. *Comput. Ind. Eng.* **2021**, *157*, 107250. [CrossRef]
215. Abualigah, L.; Gandomi, A.H.; Elaziz, M.A.; Hamad, H.A.; Omari, M.; Alshinwan, M.; Khasawneh, A.M. Advances in Meta-Heuristic Optimization Algorithms in Big Data Text Clustering. *Electronics* **2021**, *10*, 101. [CrossRef]
216. Keil, M.; Tan, B.C.; Wei, K.K.; Saarinen, T.; Tuunainen, V.; Wassenaar, A. A cross-cultural study on escalation of commitment behavior in software projects. *MIS Q.* **2000**, *24*, 299–325. [CrossRef]
217. Choi, K.-S. *Structural Equation Modeling Assessment of Key Causal Factors in Computer Crime Victimization*; Indiana University of Pennsylvania: Indiana, PA, USA, 2008.
218. Jerin, R.; Dolinsky, B.; Culture, P. You've got mail! You don't want it: Cyber-victimization and on-line dating. *J. Crim. Justice Pop. Cult.* **2001**, *9*, 15–21.