Article

Journal of Research in Crime and Delinquency
50(2) 216-238

DOI: 10.1177/0022427811425539
jrcd.sagepub.com

Online Routines and Identity Theft Victimization: Further Expanding Routine Activity Theory beyond Direct-Contact Offenses

Bradford W. Reyns[1]

Abstract

Objectives: The purpose of the current study was to extend recent work aimed at applying routine activity theory to crimes in which the victim and offender never come into physical proximity. To that end, relationships between individuals' online routines and identity theft victimization were examined. Method: Data from a subsample of 5,985 respondents from the 2008 to 2009 British Crime Survey were analyzed. Utilizing binary logistic regression, the relationships between individuals' online routine activities (e.g., banking, shopping, downloading), individual characteristics (e.g., gender, age, employment), and perceived risk of victimization on identity theft victimization were assessed.

[1] Department of Criminal Justice, Weber State University, Ogden, UT, USA

Corresponding Author:
Bradford W. Reyns, Department of Criminal Justice, Weber State University, 1206 University Circle, Ogden, UT 84408, USA.
Email: bradfordreyns@weber.edu

Keywords
identity theft, identity fraud, routine activity theory, victimization

Identity theft is a term used to categorize several offenses involving the fraudulent use of an individual's personal information for criminal purposes and without their consent. Crimes typically associated with identity theft include credit card fraud, banking fraud, and document fraud, among others. Few empirical studies of identity theft victimization have been published, but available evidence suggests that identity theft is becoming a growing problem (Baum 2007; Langton and Baum 2010; Levi 2008; Smith 2010). For instance, according to the Federal Trade Commission (FTC 2010), as many as 9 million Americans have their identities stolen each year, with a median cost to victims of $500. A recent National Crime Victimization Survey (NCVS) report indicates that 6.6 percent of all households in the United States included a victim of one or more types of identity theft, an increase of 23 percent since 2005 (Langton and Baum 2010). Citizens of the United States are not the only ones at risk of identity theft victimization. For example, a recent report by Britain's National Fraud Authority (NFA 2010) estimated that each year identity crimes affect 1.8 million British citizens and cost the United Kingdom approximately £2.7 billion. This equates to over £1,000 in financial gain from every stolen identity. Further, Levi (2008) reported that in 2006 £212.6 million in card-not-present fraud (phone/Internet/e-mail) was committed on U.K.-issued credit cards, an increase of 16 percent since 2005. These high stakes underscore the importance of identifying risk factors for identity theft victimization, many of which could be avoidable given the utility of the routine activities perspective in preventing crime.

The routine activities perspective has demonstrated its usefulness in accounting for a variety of types of criminal victimization (e.g., burglary,

larceny, stalking; Spano and Freilich 2009). Originally developed to explain changes in crime rates following World War II, the theory has since been extensively tested and strongly supported (e.g., Cohen and Felson 1979; Cohen, Felson, and Land 1980; Cohen, Kluegel, and Land 1981; Kennedy and Forde 1990; Messner and Blau 1987; Sampson and Wooldredge 1987; Wilcox Rountree, Land, and Miethe 1994). At the societal level, routine activity theory stipulates that changes in aggregate routine activities (e.g., a greater tendency to be away from the home) can create opportunities for crime. At the individual level, empirical research has also highlighted the importance of individuals' routine activities in creating criminal opportunities (e.g., Fisher, Daigle, and Cullen 2010; Fisher et al. 1998; Henson et al. 2010; Miethe and Meier 1990; Mustaine and Tewksbury 1998, 1999; Wilcox, Tillyer, and Fisher 2009).

According to the theory, criminal opportunities emerge when motivated offenders converge in time and space with suitable targets in environments lacking capable guardianship. The theoretical propositions of routine activity theory (i.e., exposure and proximity to motivated offenders, target attractiveness, and a lack of guardianship) have become the primary explanations for what puts individuals at risk of victimization. Indeed, the continued popularity of the theory in explaining direct-contact offenses (those offenses in which victims and offenders intersect in the same physical location) has prompted researchers to begin to explore the possibility of using the theory to explain opportunities for crimes occurring at a distance (those offenses in which the victim and offender never meet in the same place; e.g., Eck and Clarke 2003; Holtfreter, Reisig, and Pratt 2008; Pratt, Holtfreter, and Reisig 2010).

As Tillyer and Eck (2009) have pointed out, the theory has primarily been focused upon offenders who make contact with their targets at places. However, many crimes do not require direct contact at a physical location. This has prompted Tillyer and Eck to conclude that "Either routine activities theory is limited to place-based crimes or it needs revision" (2009:286). Early efforts to apply routine activity theory to crimes in which the victim and offender do not intersect in time and space have yielded mixed, but encouraging results (e.g., Choi 2008; Holt and Bossler 2009; Holtfreter et al. 2008; Marcum, Higgins, and Ricketts 2010; Pratt et al. 2010). These studies have focused upon online forms of victimization such as harassment, computer virus infection, and fraud victimization, and suggest that more work is needed both in identifying online routine activities that might place Internet users at greater risk of different types of online victimization, and in applying the theory to explain crimes at a distance. The current study

addresses both of these issues by examining identity theft victimization from a routine activities perspective.

Identity Theft Victimization

Although the extant routine activities literature has explored many different types of victimization, it has not yet been empirically tested on identity theft victimization. Identity theft became a federal crime in the United States in 1998 with the passage of the Identity Theft Assumption and Deterrence Act. According to this act, identity theft occurs when, knowingly and without legal authority, an individual's identity is appropriated with the intent to aid or engage in unlawful activity. Although identity theft is a complex concept that has assumed a variety of ambiguous meanings, this definition is consistent with that provided by Koops and Leenes (2006:556) who defined it as "... fraud or another unlawful activity where the identity of an existing person is used as a target or principal tool without that person's consent." Examples of identity theft based on these definitions include bank fraud, credit card fraud, and document fraud. As Koops and Leenes (2006) pointed out, the identity theft label is further complicated when the term is used synonymously with *identity fraud* (Finch 2007; McNally and Newman 2008). According to the authors, identity fraud is "... fraud committed with identity as a target or principal tool" (Koops and Leenes 2006:556). As an example, a secretary may be instructed by his or her employer to sign documents that he or she is not authorized to sign, thereby committing identity fraud. It follows then that identity theft is a category of identity fraud, but incidents of identity fraud do not necessarily constitute identity theft. The key differences between these two terms are consent and whether the identity belongs to someone.

Identity theft is a crime in which the victim and offender seldom meet face-to-face. Common methods of obtaining the victim's identity include phishing, skimming, hacking, or theft of actual identification documents (e.g., driver's license, social security card). Recent estimates of identity theft indicate that it is a growing problem and that an increasing number of cases of identity theft involve the theft of personal information via the Internet (Finch 2007; see also Levi 2008 for a discussion of card not present frauds). These cases of Internet fraud take many forms, and involve various aspects of Internet use (e.g., e-mail, banking), with offenders increasingly finding inventive ways to access their targets—the victim's personal information (Finch 2003; Newman and Clarke 2003; Smith 2010). Once the thief has the victim's stolen information, it is possible to apply for credit cards or

loans using the victim's identity, acquire a driver's license with the victim's name (but the offender's picture), or apply for government benefits using the victim's identity (FTC 2010).

Little empirical criminological research has examined identity theft victimization or investigated the factors that place individuals at risk for this type of victimization. However, recent fraud victimization studies have identified low self-control, routine activities, and victim characteristics as important correlates of fraud victimization (e.g., Holtfreter et al. 2008, 2010; Titus, Heinzelmann, and Boyle 1995; van Wilsem 2011), underscoring the need for similar work with identity theft victimization. An examination of identity theft from a routine activities perspective is far overdue, and will contribute both to the identity theft victimization literature and to the routine activities literature.

Routine Activities, Crimes at a Distance, and Identity Theft Victimization

Criminologists have long recognized that technological changes can create new opportunities for crime and victimization (e.g., Clarke 2004; Cohen and Felson 1979; Newman and Clarke 2003). For instance, Clarke (2004:55) has argued that "The Internet has created a completely new environment in which traditional crimes—fraud, identity theft and child pornography—can take new forms and prosper." Indeed, few technological innovations have had the immense impact upon societal routine activities as the advent of the Internet. According to some sources, nearly 2 billion individuals use the Internet, and in some regions of the world, a substantial portion of the population routinely accesses the Internet (Internet World Stats 2010). Recent estimates suggest that approximately 77 percent of residents of North America are online, an increase of 146 percent since the year 2000. In Europe, 58 percent of residents use the Internet, which is an increase of over 350 percent since 2000 (Internet World Stats 2010). Online criminal opportunities have kept pace with these societal changes in routine activities (Clarke 2004; Newman and Clarke 2003; Reyns 2010).

Routine activity theory explains the circumstances under which opportunities for criminal victimization occur. Originally, Cohen and Felson (1979) focused upon societal routine activities, especially a greater propensity for women to be away from the home (leaving the home unguarded), as an explanation for increased crime rates in the United States following World War II. At the time routine activity theory was introduced by Cohen and Felson (1979), the Internet did not exist, and the assumption was that most

offenses would transpire between a motivated offender and a suitable target at a physical location in the absence of capable guardians. Similar to the changes that occurred following World War II, our global society may be experiencing a shift in its routine activities—not a shift in activities away from the home per se, but a shift toward greater participation in remote activities. That is, activities that formerly required one to be physically present at a specific location, often at a specific time, can now be undertaken regardless of the individual's physical location or time of day (e.g., online classes, online shopping). Further, as such technologies continue to advance, access to the Internet and the capability to participate in these remote activities continue to grow. This growth in remote, Internet-based routine activities and the subsequent profusion of criminal opportunities has necessitated an adaptation of the theory to crimes in which the offender and target do not physically meet.

Eck and Clarke (2003:34) have suggested that routine activity theory can be expanded to explain crimes in which the victim and offender do not interact at the same physical location:

> Routine activity theory can be expanded to accommodate action at a distance by making one modification. If the target and the offender are part of the same geographically dispersed network, then the offender may be able to reach the target through the network.

In other words, although the victim and offender may not occupy or interact within the same physical location, the integrity of theory is maintained by an interaction of the victim and offender within a network. It is the convergence of motivated offenders and suitable targets within unguarded systems or networks that creates circumstances conducive to victimization. This expanded conceptualization of routine activity theory in which the network facilitates interaction between victim and offender is useful in applying the theory to identity theft victimization, as well as to other crimes in which the victim and offender never interact in the same place.

A growing body of research has investigated the role of online routine activities in explaining online forms of victimization (e.g., Choi 2008; Holt and Bossler 2009; Holtfreter et al. 2008; Marcum et al. 2010; Pratt et al. 2010). However, no study to date has empirically examined identity theft victimization from a routine activities perspective. Still, those studies examining fraud victimization, a related crime, shed light on the potential correlates of identity theft victimization. For instance, Pratt and his colleagues (2010) utilized routine activity theory to explain fraud targeting among a representative sample of Florida residents. The authors reported that both

of their measures of online routine activities, hours spent online and whether the respondent made an Internet purchase, were predictive of Internet fraud targeting. Using the same data as Pratt et al. (2010), Holtfreter and her colleagues (2008) examined the fraud targeting and victimization of Florida residents, highlighting the importance of remote purchasing behaviors (e.g., Internet purchase, telephone purchase) in both fraud targeting and fraud victimization. Further, Reisig, Pratt, and Holtfreter (2009) identified perceived risk of Internet theft victimization as an important influence on online behaviors, reporting that consumers who perceived their risk of victimization to be higher spent less time online and made fewer purchases while online.

Considering the prevalence and seriousness of identity theft, as well as the trend in criminology and victimology toward further developing and refining routine activity theory for application beyond direct-contact offenses, the current study examines identity theft victimization from a routine activities perspective. Identifying risk factors for identity theft victimization will be useful in designing situational strategies to combat this type of crime (Levi 2008; Mann and Sutton 1998; Newman 2008).

Method

Data

Data for the current study were collected in 2008 to 2009 as part of the British Crime Survey (BCS). The survey began in 1982 and is the second longest running national victimization survey in the world, behind the NCVS. Like the NCVS, data from the BCS represent both reported and unreported crimes, but unlike the NCVS, the BCS also includes a host of social, demographic, and lifestyle information about respondents (Mayhew 2010). The breadth and quality of these data has made the BCS an important source of data for criminologists and victimologists interested in testing victimization theories, particularly the lifestyle-routine activities perspective (e.g., Maxfield 1987; Sampson and Lauritsen 1990; Sampson and Wooldredge 1987).

The BCS uses a complex stratified cluster sampling design in which Postcode Address Files (PAF) are used as a sampling frame, postcode sectors are used as primary sampling units, and population density and the proportion of household reference persons in nonmanual occupations are used as stratifiers (for more detail on sampling and additional procedures, see Bolling, Grant, and Donovan 2009). Once a household is selected,

individuals within selected households are listed alphabetically by first name, and a single respondent over 16 years old is randomly chosen to represent the household. Data are collected via face-to-face interviews that are facilitated by computer-assisted personal interviewing.

The sample size for the 2008 to 2009 BCS includes 46,286 residents of England and Wales, and has a response rate of 76 percent. A weighting process to adjust for nonresponse bias ensures that the sample is representative. As Table 1 illustrates, the sample utilized in the current study includes 5,985 of these individuals.[1] This group is representative of the larger BCS sample and has the following characteristics: 53 percent female, 93 percent White, 51 percent unmarried, with a mean age of approximately 43 years old.

Measures

The primary purpose of the current study was to identify risk factors for identity theft victimization by examining specific online routine activities of respondents, their individual characteristics, and their perceptions of risk of victimization. To that end, multiple measures of these concepts were chosen from the BCS data. Table 1 provides the scales and descriptive statistics for these variables.

Dependent variable. Identity theft involves the fraudulent use of the victim's identity for the personal benefit of the thief. Two survey items were used to create a measure of identity theft. First, respondents were asked: *Have any of your cards been used without your permission or prior knowledge?* Responses to this survey item were dichotomized (0 = *No*, 1 = *Yes*). Affirmative answers indicated that the respondent had been a victim of credit card fraud, the most common form of identity theft (Baum 2007; Langton and Baum 2010). Respondents were also asked: *Have you had money taken from your bank or building society accounts in some way?* This survey item reflects whether respondents had been victims of bank or account fraud. Again, responses were dichotomized (0 = *No*, 1 = *Yes*). Based on responses to these two survey items, the respondent was identified as a victim of identity theft, meaning that he or she had experienced either credit card fraud or bank/other financial fraud. This measure of identity theft is similar to that utilized in recent administrations of the NCVS (Baum 2007; Langton and Baum 2010). It is important to point out, however, that these two survey items are not online-specific, nor do they necessarily reflect victimization within an online context. This presents a potential limitation to the results of the current study.

Table 1. Scales and Descriptive Statistics.

Variable	Scale	Range	*M* (*SD*)
Dependent variable			
Identity theft	(0 = *nonvictim*, 1 = *victim*)	0–1	.08 (.27)
Online routine activities			
Banking	(0 = *No*, 1 = *Yes*)	0–1	.49 (.50)
Shopping	(0 = *No*, 1 = *Yes*)	0–1	.65 (.47)
E-mail or IM	(0 = *No*, 1 = *Yes*)	0–1	.83 (.37)
Watch TV/radio	(0 = *No*, 1 = *Yes*)	0–1	.21 (.40)
News	(0 = *No*, 1 = *Yes*)	0–1	.32 (.46)
Chat rooms/forums	(0 = *No*, 1 = *Yes*)	0–1	.10 (.30)
Reading/writing blogs	(0 = *No*, 1 = *Yes*)	0–1	.07 (.26)
Downloading	(0 = *No*, 1 = *Yes*)	0–1	.26 (.43)
Social networking	(0 = *No*, 1 = *Yes*)	0–1	.28 (.45)
Work or study	(0 = *No*, 1 = *Yes*)	0–1	.59 (.49)
Individual characteristics			
Sex	(0 = *Female*, 1 = *Male*)	0–1	.47 (.49)
Age	(Age in Years)	16–91	43.36 (15.32)
Non-White	(0 = *White*, 1 = *Non-White*)	0–1	.07 (.26)
Married	(0 = *Not married*, 1 = *Married*)	0–1	.49 (.50)
Income	(0 = *Less than* £50,000, 1 = *More than* £50,000	0–1	.23 (.42)
Employed	(0 = *Unemployed*, 1 = *Employed*)	0–1	.69 (.46)
Away home	(0 = *Home Occupied During Day*, 1 = *Home Unoccupied During Day*)	0–1	.91 (.28)
Perceived risk			
Perceived risk	(1 = *Very Unlikely*, 2 = *Fairly Unlikely*, 3 = *Fairly Likely*, 4 = *Very Likely*)	1–4	2.33 (.77)

Note. IM = instant messaging; TV = television.
N = 5,985.

Online routine activities. As Mustaine and Tewksbury (1998) have pointed out, routine activities research has often relied on indirect or proxy measures of individuals' lifestyles and routine activities (e.g., demographics) in assessing victimization risks (e.g., Cohen and Cantor 1980; Cohen et al. 1981; Hindelang et al. 1978; Messner and Tardiff 1985). Further, recent work examining crimes in which the victim and offender are

physically separated (e.g., Internet crimes) has utilized somewhat rudimentary measures of online routine activities (e.g., time spent online) without fully exploring the activities that individuals engage in while online (i.e., direct measures of routine activities). By way of comparison to Mustaine and Tewksbury's (1998) work, the critical element in explaining victimization may not be time online (or time away from the home in Mustaine and Tewksbury's case), but unguarded online activities that expose Internet users to identity theft targeting.

In an effort to examine Internet specific routine activities, 10 online routine activities measured in the BCS were identified as potential correlates of identity theft. These include using the Internet for the following purposes: (1) online banking or managing finances, (2) buying goods or services (shopping), (3) e-mail or instant messaging (IM), (4) watching television or listening to the radio, (5) reading online newspapers or news Web sites, (6) participating in chat rooms or other forums, (7) reading or writing blogs, (8) downloading music, films, or podcasts, (9) social networking (e.g., Facebook, Myspace, Bebo), or (10) for work or study. Respondents were asked: *Which, if any, of the following things do you use the Internet for?* Responses were dichotomized (0 = *No*, 1 = *Yes*).

Offline routine activities. A final routine activities measure based on guardianship of the home was included in the analyses, as prior research suggests that this is a variable of theoretical importance (Cohen and Felson 1979; Cohen et al. 1981; Messner and Blau 1987). In the case of identity theft, important information about the victim's identity could be gained by entering the home and physically retrieving it; however, the existing research on identity crimes suggests that thieves are increasingly turning to the Internet as a means of reaching their targets (Holtfreter, Van Slyke, Blomberg 2005). This measure of home guardianship is based on the following survey item: *Is your home ever left unoccupied during weekdays?* Responses were dummy-coded (0 = *No*, 1 = *Yes*).

Individual characteristics. Individuals' personal characteristics may influence their risks of identity theft victimization inasmuch as these characteristics are linked to patterns of Internet use and victimization. For example, individual characteristics are linked to the amount of time spent online, which in turn increases likelihood of exposure to risky situations. Pratt et al. (2010) reported that the amount of time respondents spent online was a function of age, gender, and race, with males spending more time online and older persons and Blacks spending less time online. Further, Holtfreter

et al. (2008) reported that these characteristics were significant predictors of fraud victimization. Considering the connections between individuals' personal characteristics, their online routines, and victimization, six of these individual characteristics of respondents were included in the analyses: (1) sex (0 = *female*, 1 = *male*), (2) race (0 = *White*, 1 = *non-White*), (3) age (in years), (4) marital status (0 = *not currently married*, 1 = *married*), (5) income (0 = *less than £50,000*, 1 = *more than £50,000*), and (6) employment status (0 = *unemployed*, 1 = *employed*).

Perceived risk of victimization. The fear of crime literature suggests that perceived risk of victimization may constrain individuals' behavior, altering their routine activities (Reisig et al. 2009; Warr 2000). It therefore becomes important to consider the role of perceived risk in conjunction with respondents' online routine activities in influencing identity theft victimization. Theoretically, those perceiving their risk of victimization to be higher will expose themselves to fewer risky situations and have a lower likelihood of actual victimization. At the same time, individuals who have previously been victimized may consider themselves at greater risk of victimization and adjust their routines accordingly. To measure perceived risk, respondents were asked the following question: *How likely do you think you are to be a victim of bank or credit card fraud in the next year?* Answer choices included: (1 = *very likely*, 2 = *fairly likely*, 3 = *fairly unlikely*, and 4 = *very unlikely*). Respondents' answers were reverse coded for the analyses, with higher scores indicating a greater perceived risk of identity theft victimization.

Analytic Strategy

Prior to modeling the relationships between respondents' individual characteristics, online routines, perceived risk of victimization, and identity theft victimization, the possibility of multicollinearity among the predictor variables was explored. Tolerance and variance inflation factor statistics indicate that multicollinearity is not a statistical threat to the results of the study. Thus, the analyses proceeded in three stages. First, Pearson's *r* statistics were calculated in order to examine the bivariate relationships between the study variables. Second, a baseline binary logistic regression model was estimated including only respondents' individual characteristics on their victimization. Third, a full binary logistic regression model was estimated that included respondents' individual characteristics as well as their routine activities and perceived risk variables. Since prior research and theory

suggests that lifestyles and routine activities mediate the relationship between individual characteristics and victimization, this two-step modeling process allows for an evaluation of this proposition.

Table 2. Bivariate Relationships Between Study Variables.

Variables	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
Identity theft	1.00																		
Banking	.10*	1.00																	
Shopping	.07*	.39*	1.00																
E-mail/IM	.06*	.27*	.25*	1.00															
Watch TV/Radio	.02*	.21*	.19*	.15*	1.00														
News	.04*	.23*	.18*	.19*	.33*	1.00													
Chat Rooms/Forums	.02*	.09*	.09*	.09*	.23*	.15*	1.00												
Read/Write Blogs	.01	.10*	.08*	.08*	.26*	.19*	.32*	1.00											
Downloading	.04*	.19*	.18*	.14*	.30*	.19*	.24*	.21*	1.00										
Social networking	−.00	.11*	.07*	.11*	.18*	.14*	.28*	.21*	.29*	1.00									
Work or study	.04*	.16*	.12*	.16*	.17*	.23*	.08*	.13*	.14*	.07*	1.00								
Sex	.02*	.04*	.06*	−.01	.10*	.11*	.06*	.05*	.09*	−.05*	.04*	1.00							
Age	.02*	−.06*	−.03*	.01	−.15*	−.12*	−.20*	−.13*	−.28*	−.47*	−.00*	.05*	1.00						
Non-White	.00	−.04*	−.11*	−.01	.06*	.10*	.02	.03*	.00	.02*	.04*	.00	−.14*	1.00					
Married	.06*	.06*	.08*	.03*	−.03*	.00	−.10*	−.07*	−.12*	−.26*	−.02*	.07*	.31*	−.02	1.00				
Income	.07*	.17*	.18*	.12*	.08*	.17*	.01	.04*	.09*	−.01	.19*	.08*	−.06*	−.01	.20*	1.00			
Employed	.03*	.14*	.14*	.04*	.07*	.11*	.01	.03*	.07*	.03*	.18*	.09*	−.24*	−.01	.04*	.18*	1.00		
Away home	−.00	.04*	.05*	.04*	−.00	.00	.00	−.03*	.00	.00	.02	−.06*	.04*	−.05*	−.04*	.03*	−.00	1.00	
Perceived risk	.02*	.11*	.10*	.08*	.02	.03*	−.02*	.00	−.00	−.104*	.05*	−.05*	.06*	.03*	.09*	.07*	.10*	.02*	1.00

Note. IM = instant messaging; TV = television.
$N = 5{,}985$.
*$p < .05$ (two-tailed test).

Table 3. Binary Logistic Regression Coefficients, Standard Errors, and Exponentiated Coefficients for Identity Theft Victimization.

	Model 1			Model 2		
Variables	Coefficient	*SE*	Exp(*B*)	Coefficient	*SE*	Exp(*B*)
Individual characteristics						
Sex	.10	.08	1.10	.19*	.10	1.22
Age	.008*	.004	1.01	.01**	.004	1.01
Non-White	.25	.17	1.29	.12	.18	1.12
Married	.21*	.10	1.24	.17	.10	1.19
Income	.45*	.10	1.58	.24*	.11	1.27
Employed	.24*	.11	1.24	.04	.12	1.05
Online routine activities						
Banking	—	—	—	.42***	.11	1.52
Shopping	—	—	—	.27*	.12	1.31
E-mail or IM	—	—	—	.43**	.17	1.54
Watch TV/radio	—	—	—	−.12	.12	.88
News	—	—	—	.06	.11	1.06
Chat Rooms/Forums	—	—	—	.28	.16	1.32
Reading/Writing blogs	—	—	—	.01	.18	1.02
Downloading	—	—	—	.24*	.11	1.27
Social networking	—	—	—	−.09	.13	.91
Work or study	—	—	—	.02	.11	1.02
Offline routine activities						
Away home	—	—	—	.04	.18	1.04
Perceived risk	—	—	—			
Perceived risk	—	—	—	1.05***	.06	2.86
Constant	−3.19***	.20	.04	−6.08***	.39	.001
−2 Log likelihood	3,517.04			3,156.81		
Model χ^2	50.15***			410.37***		
Nagelkerke R^2	.03			.15		
N	5,985			5,985		

*$p < .05$.
**$p < .01$.
***$p < .001$.

Note

1. While the British Crime Survey (BCS) includes information on over 46,000 respondents, only a subsample of this group was examined in the current study. Respondents who were randomly selected to answer *module d* of the survey were selected for inclusion in the current analyses (this module included data on perceived risk of victimization). Of these, complete data were available for 5,985 respondents.