10-20-2020

Situational Awareness and Public Wi-Fi Users' Self-Protective Behaviors

David Maimon
Georgia State University

C. Jordan Howell
Georgia State University

Scott Jacques
Georgia State University

Robert Perkins
Georgia State University

Situational Awareness and Public Wi-Fi Users' Self-Protective Behaviors

David Maimon[1], C. Jordan Howell[1], Scott Jacques[2], Robert Perkins

[1]Georgia State University, [2]Criminology Open and Georgia State University

Published on: Oct 20, 2020

Updated on: Oct 29, 2020

DOI: 10.21428/cb6ab371.b687013c

ABSTRACT

Accessing public Wi-Fi networks can be as dangerous as it is convenient. People who access a public Wi-Fi network should engage in self-protective behaviors to keep their data safe from malicious actors on the same network as well as persons looking over their shoulder, literally and proverbially. Using two independent research designs, we examined under what circumstances were people more likely to access an unsecured Wi-Fi network and engage in risky behavior on these networks. Findings from the first study, based on survey data, reveal that people who are more situationally aware are less likely to access personal accounts on public Wi-Fi, and more likely to cover their screen to prevent others from viewing personal information. Additionally, findings show that people with higher computer proficiencies are less likely to engage with public Wi-Fi. For the second study, our research team designed and deployed honeypot Wi-Fi networks. We found that people are more likely to access these unsecured, rogue networks in establishments with fewer on-duty employees and that do not offer legitimate public Wi-Fi. Additionally, the number of on-duty employees is associated with an increase in physical security behaviors, such as concealing a screen. We conclude by discussing how these findings can aid in reducing susceptibility to online victimization.

Introduction

Public Wi-Fi networks provide a convenient, cost-effective way for accessing the Internet in areas where a wired infrastructure is challenging. This convenience resulted in public Wi-Fi networks appearing in public places in substantial numbers in recent years. In most cases, these wireless networks do not require any form of user authentication or identification for using them (Zafft and Agu 2012). This makes users vulnerable to privacy and security attacks. Additionally, wireless signals leak beyond buildings in which access points are installed, so intruders can pick up these signals from parking lots or nearby buildings (Zafft and Agu 2012).

A recent global survey found that among one hundred information technology security leaders, nearly three-fourths report that they suffered a breach as a result of a mobile security issue, with thirty percent of the breaches caused by unsecured wireless connections (Cockerill 2015). Another study found that ninety-two percent of Americans have put personal information at risk, including their bank account details, by transferring sensitive information over public Wi-Fi (Norton 2017).

Users are often encouraged to restrict their web traffic to information that is not considered sensitive (e.g., avoid submitting financial information, usernames, and passwords). For instance, the Federal Trade Commission (FTC) encourages public Wi-Fi users to take specific precautions while using these networks. Users are instructed to use encrypted Wi-Fi networks, only enter personally identifiable information on secured networks, use Virtual Private Network (VPN) connections, and avoid sending

emails containing personal information (Rouge 2017). A few experts go further, suggesting that since malicious Wi-Fi networks could be easily deployed by criminals (Zafft and Agu 2012), users should completely avoid online banking and accessing sensitive data over a public Wi-Fi network, even if these websites are encrypted (Conti et al. 2016). Many websites that request users to submit sensitive data use Hypertext Transfer Protocol Secure (HTTPS) to ensure transferred data is encrypted. However, HTTPS over a public Wi-Fi network can be compromised relatively easily and is not recommended as a complete security solution (Krebs 2012).

Despite the continued efforts to improve public Wi-Fi users' awareness of these hazards and the security measures that they need to take (Holt and Bossler 2014; Norton 2017), a significant amount of users continue to put their security at risk by submitting sensitive data both in public and over unsecured Wi-Fi networks (Norton 2017). The security threat is particularly significant while using public Wi-Fi networks because users must contend with potential offenders on the same network and in the public space around them (Eiband et al. 2017), which are respective instances of "online" and "offline" behaviors.

Regarding the latter, "shoulder surfing" is observing other people's information without their consent (Eiband et al. 2017). This has become a much greater threat due to the prevalence of mobile phones equipped with cameras and video recorders (Eiband et al. 2017). Thieves can covertly snap pictures of credit cards, credit applications, or record entire conversations while appearing to be texting or talking on the phone (Brudy et al. 2014; Honan 2012). At its core, protective behavior involves positioning the screen so that information is not viewable by others (Brudy et al. 2014). The literature shows that self-protection is effective at preventing victimization (Bachman et al. 2002).

Situational Awareness (henceforth SA) includes being mindful of the surroundings and identifying potential threats and dangerous situations. It may be important in determining network users' adoption of self-protective behaviors, and consequently mitigating the threat of online crime over public Wi-Fi networks. Specifically, it is possible that being aware of the physical surroundings plays into a person's decision-making and threat perception (Endsley 1995; Klein 1989) and leads to self-protective behaviors.

This article examines SA in shaping public Wi-Fi users' adoption of self-protective behaviors while using public networks, including whether environmental cues (e.g., place managers or on-duty employees) encourage users to be more aware of their security and be more protective. We draw on the Situational Crime Prevention (SCP) perspective to understand how users protect themselves while using public Wi-Fi networks. We consider whether SA and place management can be used to increase our understanding regarding peoples' decisions to employ self-protective behaviors while using public Wi-Fi networks.

The next section introduces the relevance of self-protective behaviors in reducing people's likelihood of becoming a crime victim. It also discusses the impact of SA and place management on both online and offline self-protective behaviors. That is followed by a description of the two studies we conducted. Finally, the results are presented and discussed.

Theoretical Background

Victim Self-Protective Behavior

Broadly speaking, criminologists differentiate between two major types of Victim Self-Protective Behavior (VSPB): forceful and non-forceful resistance. Forceful resistance refers to active aggressive behaviors like pushing, biting, and kicking, that are introduced by a victim directly against a perpetrator in order to prevent an act of crime (Ullman 1997). Non-forceful resistance, on the other hand, refers to passive resistance techniques that are used by a victim to avoid offenders, and consequently, reduce the probability of a criminal event (Guerette and Santana 2010). Examples of behaviors that could be classified as non-forceful strategies include avoiding an offender, escaping, pleading, and begging. A majority of VSPB research has focused on types of self-protective behaviors that are most effective in preventing rape completion (see Ullman 2007 for a review of the literature), other studies demonstrate how resistance can decrease the likelihood of other forms of victimization such as domestic violence (Bachman et al. 2002) and robbery (Guerette and Santana 2010; Ziegenhagen and Brosnan 1985) from being completed.

More recently, scholars have examined self-protective behaviors employed by victims of various forms of cyber abuse. Fissel (2018) operationalized self-protection as reporting victimization experiences to the police, whereas Worsley et al. (2016) focused on the psychological impacts of victimization and conceptualized self-protective behaviors as the implementation of various coping mechanisms. Lastly, Sheridan and Grant (2007) identified the following self-protective behaviors that people engage in when experiencing cyberstalking: changing employment/course of study, getting rid of car, increasing security, changing identity, and giving up social activities. Although the literature is expanding to include self-protective behaviors used in online environments, Nobles et al. (2014, p.993) accurately state the literature "has not developed to the point where patterns in responses to victimization, including self-protective behaviors taken by the victim, have been clearly identified."

The dearth of literature is evident when examining VSPB for more technical forms of cyber victimization. One environment in which Internet users are susceptible to victimization experiences is when using public Wi-Fi networks. Although criminologist have done little to examine how users of public Wi-Fi networks mitigate the risks of untrusted networks, several protective or coping behaviors have been identified that reduces one's risk of being victimized (Klasnja et al. 2009). These tend to be solutions in which people can engage in the physical world (i.e., concealing their devices, ensuring that others are not sitting immediately next to them, or being cognizant of potentially suspicious people

around them (Klasnja et al. 2009)) or in cyber space (i.e., using remote VPN or avoiding accessing personal information while on the network). Increasing such behavior and reducing risk-taking behavior is of crucial importance for preventing the completion of criminal events (Bachman et al. 2002). Thus, getting users to reduce their risk online by protecting themselves and their data while using public Wi-Fi networks is a key element of reducing vulnerability to cybercrime (Watts 2016). This assumption is consistent with Clarke's SCP framework (Clarke 1980).

Situational Crime Prevention

All in all, the SCP perspective is a preventive approach to crime that relies upon reducing opportunities for crime by focusing on the relationship between the offender and the actual environment in which the crime takes place. It is a general approach as well in reducing opportunities for any kind of crime occurring in any kind of setting (Clarke 1995). The underlying premise of this perspective is that criminals are rational beings who weigh the costs and benefits of their prospective behaviors. Therefore, successful crime prevention efforts must involve the design and manipulation of human environments to make offenders' decisions to get involved in crime less attractive (Herath and Rao 2009). Drawing on the routine activities perspective assumption that opportunity is a root cause of crime (Cohen and Felson 1979), Clarke (1980) proposes that crime can be prevented by reducing criminogenic opportunities in the environment. The opportunity-reducing methods of SCP fit systematic patterns and rules which cut across every walk of life, even though prevention methods must be tailored to each situation. These methods aim to: increase the perceived effort of crime; increase the perceived risks; reduce the anticipated rewards; prevent provocations; and remove excuses for crime. For example, reducing rewards entails avoiding sending personal information and avoiding accessing sensitive websites, such as banking websites, over public Wi-Fi networks (Reyns 2010). Increasing the effort for cyber criminals can be accomplished by avoiding accessing unknown public Wi-Fi networks, restricting the submission of personal information over Wi-Fi networks, and by the owners of the public Wi-Fi setting a password to access the network.

VSPBs in its various forms are of relevance in the context of this perspective since victims' resistance would increase offenders' efforts to complete a criminal event and offset offenders' cost and benefit calculations (Guerette and Santana 2010). Moreover, victims' use of non-forceful resistance techniques like evasion and avoidance, in both online and offline situations, will remove the victim from the criminogenic situation, and prevent the occurrence of a criminal event (Ziegenhagen and Brosnan 1985). However, we believe that the implementation of self-protective behaviors is dependent on potential targets' awareness of their environment (i.e., their level of SA).

Situational Awareness

SA is pertinent to people who find themselves in threatening situations (Rozee and Koss 2001). The concept refers to adaptive, externally directed consciousness (Smith and Hancock 1995). SA generates

behavior to achieve a goal in a specific task environment. Its products are knowledge about and directed action within that environment (Smith and Hancock 1995). Most importantly, SA endows the competence to generate appropriate behavior in response to complex and dynamic situations (Cohen and Felson 1979; Klein 1989). This competence is based on long-term memory structures that allow people to quickly understand a given situation: A person has prototypical situations in one's memory, with each corresponding to a "correct" action. Thus, in an unfolding situation, a person determines how to act by matching its characteristics to a prototypical situation. SA, to be clear, is not a constant across people. Some people demonstrate more of it. This may be a function of a person's information-processing mechanisms as influenced by innate abilities, experience, and training; or, may reflect preconceptions and objectives that filter and interpret the environment (Endsley 1995).

Place Management

The SCP perspective, as stated above, is comprised of measures "(1) directed at highly specific forms of crime (2) that involve the management, design, or manipulation of the immediate environment in as systematic and permanent a way as possible (3) so as to reduce the opportunities for crime and increase its risks as perceived by a wide range of offenders" (Clarke 1983, p. 225). One of the original strategies proposed by Clarke (1980) to reduce the occurrence of crime involves the introduction of surveillance means. According to Clarke, the introduction of guardians and surveillance means in the environment may mitigate crime by increasing offenders' perceived threat of detection and punishment. In general, Clarke and Homel (1997) identify three types of surveillance: natural surveillance, formal surveillance, and surveillance by place managers (or surveillance by employees). Natural surveillance involves the manipulation of the physical environment in order to improve a person's ability to observe the environment and increase the chance of offenders being detected when committing a crime (Welsh et al. 2010). In the offline environment, this can be accomplished by improving street lighting and promoting the "see something, say something" agenda. Formal surveillance involves the introduction of official forms of crime prevention personnel, such as police officers, security guards, and crime prevention hardware such as CCTV cameras, red light cameras, and burglar alarms (Clarke 1997). Lastly, surveillance by place managers involves the use of employees who have non-security related responsibilities in an organization to also fulfill a surveillance role (Chen and Zahedi 2016). Such personnel include building attendants, concierges, park keepers, train conductors, and convenience store clerks. A place managers primary responsibility is not to reduce crime, but to ensure business operates smoothly through the management of social and physical characteristics (Madensen 2007). However, these characteristics are also essential for crime prevention, and effective place managers can reduce the opportunity for people to engage in crime.

If networks are places, then network administrators, designers, and facilitators are their place managers (Reyns 2010). Managers of online places have a particularly important role in the prevention of cybercrime especially when considering public Wi-Fi networks due to their nature (i.e., completely

open physically and virtually). Network place managers potentially have great control over what transpires within their networks and domains. In addition, they can limit access and set rules for participation on the network. As such, their role in preventing online crimes is of paramount importance (Reyns 2010).

Further, public Wi-Fi networks have criminogenic properties which make cybercrime possible by providing easy opportunities for the crime to occur. Newman and Clarke (2003) describe elements of information systems that are themselves conducive to crime using the acronym SCAREM. SCAREM stands for Stealth (Internet users can effectively remain invisible while online), Challenge (e.g., hacker's may enjoy the challenge presented by online crime); Anonymity (online environments are inherently anonymous); Reconnaissance (the interconnected nature of the Internet makes it possible for offenders to scan thousands of servers or computers for loopholes to exploit); Escape (the stealth and anonymity aspects of online domains make it easier for offenders to avoid detection); and Multiplicity (online domains provide multiple targets). It can be argued that public Wi-Fi networks have the criminogenic qualities of SCAREM. For example, public Wi-Fi networks provide not only fertile ground for cybercrime to take place (e.g., provides offenders with stealth, reconnaissance and escape), but also a wealth of potential victims – all users of the network (multiplicity).

As discussed at the beginning of this section, surveillance can increase offenders perceived threat of detection and punishment. Place managers can reduce the attractiveness of a location for criminals (i.e., parking lot attendants can alert you of a recent spate of car thefts in the area and encourage you to lock your car). Likewise, hotel concierges can alert you to dangerous areas in the vicinity. By using place managers in the location of the public Wi-Fi network as sources of information and providers of surveillance, users have a point of contact if they have queries about using the public Wi-Fi network (i.e., employees of a public Wi-Fi location can be approached and questioned as to whether there is a password for the public Wi-Fi network or whether a specific network that the user is picking up is associated to the location or not). Thus, place managers help potential victims avoid the temptation of accessing potentially malicious networks in the vicinity. Although the idea of place managers being used to prevent the occurrence of crime has a rich theoretical development, it has not been subject to rigorous evaluation research (Douglas and Welsh 2020). In fact, in a systematic review on alternative measures of surveillance, Welsh and colleagues (2010) only identified two high-quality evaluations of the effectiveness of place managers at reducing crime. However, neither of these examinations assess the effectiveness of place managers at reducing the opportunity of online crime.

Hypotheses

Based on the above concepts, theories, and findings, we expect to find that when potential public Wi-Fi users exhibit greater SA, they are more likely to: 1) Be aware that a public Wi-Fi network is available at a place; and 2) Engage in more self-protective behaviors while using the public Wi-Fi network. In

addition, we expect that public Wi-Fi users in places with more place managers will be enabled to engage in more self-protective behaviors. Stated as hypotheses:

H_1. *People with higher SA are more likely to use public Wi-Fi networks.*

H_2. *People with higher SA are more likely to use self-protective behaviors related to their use of public Wi-Fi networks.*

H_3. *People in places with more place managers are more likely to use self-protective behaviors related to their use of public Wi-Fi networks.*

Analytic Design and Results

To test our research hypotheses, we collected data using two unique research designs. The first study applied a survey methodology on university students' computer and network usage to assess the first two research hypotheses. To answer the third hypothesis, we implemented a field study that allowed for the collection of public Wi-Fi network packet data across a chosen United States (US) state. All statistical analyses in both studies were estimated using Stata/IC, version 15.1 (StataCorp LLC). We now present the analytic strategies and results of the two studies.

Study 1

The first study consisted of a year-long survey conducted on the campus of a large US university and was approved by the University of Maryland Institutional Review Board (350485-1). The survey was designed to ask students about their computer and network usage, focusing on areas that could potentially compromise the security and integrity of their systems as well as the security of the network to which their systems are connected. Students in large introductory courses were recruited. During recruitment, all potential participants were explained that participation in the study is completely voluntary. Those who volunteered were given a hard copy of the survey and time, in class, to fill it out. Our questionnaire was administrated during the academic years of 2014-2015 to 820 students. Once the data were cleaned, 749 responses were available for analysis.

Dependent Measures

Three dependent measures were constructed from the survey data: *Uses Public Wi-Fi Network*; *Check Online Personal Accounts on Public Wi-Fi Network*; and *Conceal Device Screen While Using Public Wi-Fi Network*. The first variable, *Uses Public Wi-Fi Network,* indicates whether the respondent uses a public Wi-Fi network. If the respondent did connect to a public Wi-Fi network, they received a value of 1, and if not, they received a value of 0. Next, *Conceal Device Screen While Using Public Wi-Fi Network* indicates whether the respondent actively attempts to hide or position their computer screen out of sight of the people around them while using a public Wi-Fi network. Those who reported actively concealing their

screen received a value of 1, those who did not received a value of 0. The third variable, *Check Online Personal Accounts on Public Wi-Fi Network,* indicates whether the respondent uses a public Wi-Fi network to check personal accounts online (0=No, 1=Yes), such as bank accounts or email accounts. This measure is our proxy for online self-protective behaviors.

Independent Measures

Independent measures captured respondents' SA and sociodemographic characteristics. *Situational Awareness* is a single item measure indicating the extent to which respondents were attentive of their surroundings while using a public Wi-Fi network. Respondents were presented with the following question. "Are you aware of the people around you when you are surfing the Internet while using a public wireless Internet hotspot?" Response options ranged from 1 (Not aware) to 5 (Very aware). We also constructed key control measures including *Male (*1=Male 0=Female*), Age* (In years), *Annual Income* and *Programming Experience*. *Annual Income* was ordinally measured using the students' self-reported income with response options ranging between 1 (Below $20,000) to 12 ($220,000 and above). The *Programming Experience* variable was ordinally measured as well and is used as a proxy measure to assess a respondent's proficiency with computers. Response options ranged between 0 (No experience) to 3 (Fluent in at least one programing language).

Analytic Strategy

First, we present descriptive statistics for the variables of interest. Next, we estimate the relationships between our list of dependent and independent variables using a series of Logit models, while controlling for potentially relevant demographic characteristics. Logit models are used to estimate the relationships between a list of independent variables and a dependent variable that is binary (0/1) in form.

Results

Table 1 presents descriptive statistics on the variables constructed from the survey data. As shown in the table, of the 749 respondents, 23% used public Wi-Fi networks, and 88% concealed their computer screens while using public Wi-Fi networks. Additionally, 43% of the respondents who used public Wi-Fi checked personal accounts online on the public Wi-Fi network. Over 65% of respondents claimed to be aware of the presence of other people in the vicinity while using a public Wi-Fi network. Reflecting the fact that the survey was conducted on at a large US university, respondents' average age is 19.60. Furthermore, nearly half of the respondents are male (49%), and 90% reported an income of less than $20,000.

--Table 1 About Here--

Table 2 presents findings estimated from the logit regression analyses. Model 1 of Table 2 reports the logit regression results for all participants in the survey (n=749). In Model 1, we see the mean effect of SA on the probability that the dependent variable takes a value of 1 (i.e., respondents use public Wi-Fi networks) is positive and marginally significant ($p<0.10$). Male respondents appear to trust public Wi-Fi networks less ($p<0.05$). Programming experience has a negative impact on the probability of using public Wi-Fi networks ($p<0.05$). That is, respondents who are more proficient with computer programming languages reported using public Wi-Fi networks significantly less. Model 2 of Table 2 shows that respondents who are situationally aware do not check personal accounts when using public Wi-Fi. Again, this result is marginally significant ($p<0.10$). However, respondents with programming experience are much less likely to check online personal accounts while using public Wi-Fi ($p<0.01$). Model 3 of Table 2 shows that respondents who are situationally aware are more likely to conceal their screens while using a public Wi-Fi network ($p<0.01$).

--Table 2 About Here--

Table 3 presents re-estimated results that were generated from Table 2's Models 3 and 4 to assess the robustness of these earlier findings. This was accomplished by restricting the analyzed sample to the respondents who admitted to using public Wi-Fi networks (n=164). Model 1 of Table 3 suggest that respondents who both use public Wi-Fi networks and practice situational awareness are less likely to check personal accounts online ($p<0.10$). This finding is marginally significant. Similarly, Model 2 of Table 3 shows that respondents who are situationally aware are more likely to conceal their screens when using public Wi-Fi ($p<0.10$). This finding is also marginally significant.

--Table 3 About Here--

Study 2

The second study consisted of a separate data collection effort. The following procedure was approved by the University of Maryland Institutional Review Board (402261-1). Specifically, we set up our own private Wi-Fi network at 109 coffee houses, restaurants, and hotels around the state of Maryland. We chose businesses that were relatively homogenous in size and customer profile (i.e., users of smart phones and/or laptops in order to reduce the possibility of an omitted confounding effect) while using a list of businesses obtained from the Maryland Department of Commerce. All selected business were located less than 60 miles away from University of Maryland campus. We collected data at each business at three periods in a day (*Morning*, *Afternoon*, and *Evening*), for one hour during each period. Due to hours of operation, we were not always able to visit each location three times in a single day. Five students (one per location) were tasked as research observers and were assigned with the task of attending each business and setting up our network. These students went through an hour-long

training session in which they were explained how the network should be set up and how they should check its functionality.

When a person would look for available Wi-Fi networks, ours appeared as an available, but private, connection. It was labeled as "private" and, thus, potential users knowingly trespassed on an unknown private network. There were no authentication requirements to join. Some, but not all, businesses offered an accessible public Wi-Fi network to guests. At the establishments which made it available, people could see the business' Wi-Fi network and our unknown private Wi-Fi network. When searching for a connection, users are able to view all Wi-Fi networks within range of connection, meaning other networks not belonging to the business or our research team were also viewable in some instances.

We collected data over a 16-month period between August 2015 and December 2016. Upon arrival at a given business, we set up our private Wi-Fi network and collected data on the physical space. Data collection included a simple count of the number of customers and employees in the location throughout the one-hour long session. Figure 1 is an example diagram of the physical location and the type of physical space data collected during each period. The diagrams contain information on the space's physical traits, including the shape of the room, the number of entrances and exits, the size and positioning of tables and seats, and any employee-only areas of the location. Figure 1 also contains information on all people in the space, including the number of them; and, for each person, their perceived gender, whether an employee or guest, possession of devices-in-use, movement through and use of the space, arrival and departure times.

--Figure 1 About Here--

Sample

We visited 109 businesses but excluded 29 of them from analyses. The excluded businesses were in city centers, train stations, and museums that, due to their busyness, proved too difficult to reliably collect data on. With those excluded from the sample, we were left with 208 one-hour sessions (duration one hour) at 80 businesses. The average location had 20 people total during the one-hour session (Min=1, Max=58). On average, 17 of these people were customers (Min=1, Max=58), and 2.73 were employees (Min=1, Max=12). The mean number of laptops is 2.30 (Min=0, Max=42.33) and the mean number of visible mobile devices is 3.30 (Min=0, Max=22).

Dependent Measures

When examining the data, we were interested in offline and online VSPB. To measure online VSPB, we constructed a dummy variable entitled *Accessed Unknown Wi-Fi Network,* taking the value of 1 if someone accessed our network, and 0 if they did not. If the private and unknown network was accessed, risky behavior was demonstrated by the user. Our measure of offline VSPB is *% Devices*

Concealed. It captures the percentage of people (within the one-hour session) who concealed their devices by positioning their backs immediately to the wall or sitting more than one chair away from other potential network users (employees excluded).

Independent Measures

Six independent variables were measured in our second study: *% Employees; % Male; Morning; Afternoon; Evening;* and *Other Network*. The first independent measure *% Employees* shows the percentage of total occupants in any given business location that were employees of that location. The *% Employees* variable includes the total number of employees present at any time during our one-hour session. Similarly, we constructed *% Male*, which is the percentage of total male occupants in any given business location during our one-hour session. We also constructed three dummy variables to capture the time of day. The variable *Morning* took the value of 1 if the session took place in the morning time (8:00 a.m. – 11:00 a.m.) and 0 otherwise. Likewise, the variable *Afternoon* (12:00 p.m. – 2:00 p.m.) took the value of 1 if the session took place in the afternoon and 0 otherwise. Lastly, the variable *Evening* (5:00 p.m. – 8:00 p.m.), which is used as the reference category, took the value of 1 if the session took place in the afternoon and 0 otherwise. To capture availability of other public Wi-Fi networks available at the business, we constructed a dummy variable entitled *Other Network*. This measure took the value 1 if another Wi-Fi network was available in the business and the value 0 if no other Wi-Fi networks were available.

Analytic Strategy

We use Hierarchical Linear (HLM) and Hierarchical Generalized Linear (HGLM) Models (Raudenbush and Bryk 2002) to capture the effect of independent measures on VSPB with respect to public Wi-Fi networks. Overall, multilevel modeling allows for the analysis of individual behaviors within larger units of aggregation (i.e., neighborhoods, schools, organizations, etc.) and addresses two potential biases that may occur when applying ordinary regression techniques to clustered data. First, it allows for more accurate estimates of standard errors when cases are clustered (and potentially correlated) within larger units. Second, it provides estimates of the impact of cross-level interactions between the larger unit of aggregation characteristics and individual-level factors. Since our private Wi-Fi network observations are embedded within place, we use two-level linear models to predict the volume of concealed computer screens, and two-level logit models to estimate public Wi-Fi users' probability to access the private and unknown Wi-Fi network (Raudenbush and Bryk 2002). For each type of analysis, we specify the observation data (Level 1), while allowing for the intercept to vary across places (Level 2).

Results

Table 4 presents descriptive statistics for the variables constructed using online and offline observations. In 16% of the one-hour sessions, our private Wi-Fi network was accessed by persons at

the business. The average percentage of people who concealed their screen in these businesses was 9.19%. The average percentage of employees (versus customers) across businesses was 20.76%. Males and females visited the businesses at nearly even rates, with males making up nearly half (48.88%) of the population. Most of the businesses (80%) provided a Wi-Fi network (*Other Network*) for guests to access.

--Table 4 About Here--

Table 5 presents results from the multilevel linear and logit regression analyses. For Model 1, the estimates show that the effect of *% Employees* on the probability that the dependent variable takes a value of 1 (respondents access an unknown private Wi-Fi network) is negative (-6%) and significant ($p<0.05$). Thus, the higher the percentage of employees (versus guests) in a location, the higher the level of online VSPB. Model 2's estimates, which adds control variables, imply a similar effect of the *% Employees* on respondents accessing a private and unknown Wi-Fi networks (-7%) and is significant ($p<0.01$). In addition, these estimates show that the effect of *Other Network* on the probability of accessing unknown networks is negative (-26%) and significant ($p<0.05$). Therefore, the higher the percentage of employees (versus guests) in a location and the ability to access other publicly available networks (versus no other publicly available networks), the higher the level of online VSPB.

--Table 5 About Here--

For Models 3 and 4 of Table 5, the mean effect of the *% Employees* measure on the percentage of users concealing the device screens *(% Devices Concealed*) is positive and significant ($p<0.05$). These model estimates suggest that a higher proportion of employees to guests makes the latter more likely to conceal their devices. Additionally, Model 4 shows that being male increases the likelihood of a person concealing their device ($p<0.05$). From these results, we see overall that more employees relative to guests leads to more offline and online VSPB.

Discussion

The Internet facilitates ways for criminals to easily access valuable information. With occurrences of cyber-criminality on the rise year after year (Norton 2017) and hackers attacking computers and networks at a near-constant rate (Cukier 2007), in conjunction with law enforcements' inability to combat these occurrences (Burruss et al. 2019), it is increasingly important to find ways to mitigate cyber-crime. Public Wi-Fi networks are often unsecured, which make their users vulnerable to attacks. Worse yet, most users of these public Wi-Fi networks believe their information is safe while using them (Norton 2017). This unawareness increases the chance of users becoming online victims (Balebako et al. 2011).

In this article, we contribute to the (cyber-)criminological literature by providing insight into whether users of public Wi-Fi networks are aware of the risks and use online and offline VSPB. We share findings from two studies, the first being survey-based and the second a field study, used to test three hypotheses. As detailed above and discussed below, findings support all three hypotheses. In line with the first hypothesis, we find that people who are more situationally aware are more likely to use public Wi-Fi networks. In support of our second hypothesis, we find that users of public Wi-Fi who exhibit SA are significantly more likely to conceal their devices and significantly less likely to visit email and banking websites when using a public Wi-Fi network. In other words, situationally aware people are more likely to engage in VSPB.

These findings indicate that SA is vital to VSPB. It follows that a practical implication of the results is that raising SA should reduce online victimization. SA training could be incorporated into computer training efforts, for example. Additionally, SA could be raised in the immediate by posting notifications in the vicinity of public Wi-Fi networks. To ensure people understand the risk, such training and notices should specify that public Wi-Fi networks put their data at risk.

The second study tested our third research hypothesis. Using a field study, we examined whether the higher the percentage of employees (place managers) in a public Wi-Fi network location increased the VSPB of Wi-Fi users. We find that more employees relative to guests is associated with less use of our private Wi-Fi network and more device concealment.

These findings demonstrate the importance of employee or place manager presence because it increases the likelihood of people not only protecting themselves offline by concealing their screens but also protecting themselves online by avoiding unknown networks. It could be that this relationship is explained because more employees makes it easier to obtain the business' Wi-Fi network password or confirm the Wi-Fi network's legitimacy. Moreover, this social milieu could lead public Wi-Fi users to be more sensitive to or otherwise aware of risk, making them less likely to access our network. A further explanation is that because our Wi-Fi network was marked private, people in its vicinity were more fearful of trespassing when there was a proportionately larger number of employees surveilling the location. In regard to offline behavior, the presence of employees may make the location more crowded, which could incentivize users to better protect themselves physically from observation attacks by protecting their screens; alternatively, employees may advise the users of such actions.

From testing these hypotheses, we uncovered other interesting patterns. People who were more proficient with computers (programming experience) reported using public Wi-Fi significantly less (50%). Perhaps those with computer skills are more familiar with the associated risk, and thus avoid public Wi-Fi networks in favor of other options such as personal Wi-Fi hotspots. This finding indicates that the more users become proficient with computers, the more aware they are of the risks involved

in using them. This can help organizations when trying to identify, and thus prioritize, which employees are in most need of security training.

Finally, in our second study, we see that when a business offers a Wi-Fi network in their location for their customers, the likelihood of those users utilizing an unknown Wi-Fi network in that location is significantly reduced. Therefore, it may be worthwhile for governments or businesses to consider installing their own secure public Wi-Fi networks in locations where users would expect Wi-Fi networks. This can be done to reduce the occurrence of Wi-Fi users availing of unknown Wi-Fi networks in public places and putting themselves at risk.

Implications for Research

These findings substantiate and extend three sets of criminological inquiry: the relevance of the SCP perspective in understanding how to reduce attacks on users of public Wi-Fi (Chen and Zahedi 2016; Clarke 1997; Reyns 2010; Welsh et al. 2010); the types of users that employ VSPB while using public Wi-Fi (Bachman et al. 2002; Klasnja et al. 2009; Watts 2016); and, the environmental cues that encourage VSPB (Bachman et al. 2002; Klasnja et al. 2009; Watts 2016). Additionally, we answer Douglas and Welsh's (2020) call for additional research into the effectiveness of place managers at reducing opportunities for crime. Moreover, the findings contribute to the information security literature that has investigated cyber security from various perspectives (Anderson and Agarwal 2010; Wright et al. 2014; Wright and Marett 2010; Xiao and Benbasat 2011). In particular, we show the need to understand how Internet users protect themselves from physical and virtual security threats in the context of public Wi-Fi use (Bachman et al. 2002; Brudy et al. 2014; Klasnja et al. 2009). We extended this vein of research by extending the focus to offline VSPB in mitigating observation attacks, such as shoulder surfing.

Implications for Practice

This work also carries practical implications for providers of public Wi-Fi networks. These organizations should promote guests' awareness of whether the business offers Wi-Fi access and, if so, how to access it (e.g., its name and password). Our findings suggest this will naturally result from having more employees on site, though it could be promoted through signage. Furthermore, practical implications for organizations stem from the finding that more proficient computer users engage in more online and offline VSPB. Training and education in technology can help people become more aware of their security. This should be sure to include – and expanded as needed – information on the types and techniques of online and offline VSPB useful for preventing attacks related to the use of public Wi-Fi networks.

Governments across the world are turning to the idea of nudging people into making safer decisions in many aspects of life. In fact, some governments are creating 'nudge units', due to growing recognition

that almost every policy issue has a human-behavioral aspect at its core. For example, the Social and Behavioral Sciences Team (SBST) of the US government was founded to use insights from psychology, behavioral economics, and other decision sciences to improve federal programs and operations. Similar teams are found in Canada, Germany, Israel, New South Wales, Singapore, and the UK (Halpern 2015; Marron 2015). Our findings suggest that the idea of nudging people into making safer decisions is applicable in not only physical spaces, but also cyberspace.

Limitations

Although the findings presented above have theoretical and policy implications, both studies have notable limitations. Our first study, which employed a sample of college students in Maryland, suffers from issues related to omitted variable bias, external validity, response bias, and the inability to establish causal relationships. It is likely that other variables, which are not included in the model, influence behavioral patterns while using public Wi-Fi networks. In this case, the coefficients and standard errors presented are bias. Additionally, we employ a relatively small sample of college students attending the same university in the state of Maryland. It is likely, and even probable, that findings drawn using such a sample are not generalizable to the national population. It is also possible that our respondents did not answer the survey questions truthfully. They may have purposefully provided falsified information or simply provided misinformation by mistake. Lastly, the cross-sectional nature of our study prevents estimating causal relationships.

Our second study, which utilizes field data, also suffers from notable limitations. Similar to the first study, we utilize cross-sectional data, which limits are ability to make causal statements. Additionally, the findings presented reflect the behavior of public Wi-Fi users within a 60 mile radius of the University of Maryland campus. It is unclear if these findings are generalizable to public Wi-Fi users in other locations. One may also argue the study suffers from issues concerning ethics. The research team did not request permission from the managers of the businesses in which the Wi-Fi networks were deployed, nor did we request consent from the people visiting the establishment during our observations. However, neither our research team nor the institutional review board viewed this as an ethical issue since personally identifiable data was not collected. Moreover, the estimated models likely suffer from omitted variable bias. Relatedly, our measures of SA are restricted to people being aware of their surroundings (i.e., being aware of the presence of place managers in a location).

Building upon the current study, research should examine whether the presence of physical items within an environment, other than people, increases VSPBs. Such items include physical notifications/signs, both in the online and offline environment. As alluded to above, signage may remind or alert people to increase their security measures (i.e., be aware of who is sitting or standing nearby, do not send sensitive information over public Wi-Fi networks, or there is no public Wi-Fi network associated with the location in question). Offline and online signs act as deterrents to persons

who may engage in risky behavior (Howell et al. 2017; Jacques 2019; Maimon et al. 2014). Future research could investigate whether a similar effect occur in in the context of Wi-Fi networks.

References

Anderson, Catherine L., and Ritu Agarwal. 2010. Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions. *MIS quarterly* 34 (3): 613-643. https://doi.org/10.2307/25750694.

Bachman, Ronet, Linda E. Saltzman, Martie P. Thompson, and Dianne C. Carmody. 2002. Disentangling the effects of self-protective behaviors on the risk of injury in assaults against women. *Journal of Quantitative Criminology* 18 (2): 135-157. https://doi.org/10.1023/A:1015254631767.

Balebako, Rebecca, Pedro G. Leon, Hazim Almuhimedi, Patrick Gage Kelley, Jonathan Mugan, Alessandro Acquisti, Lorrie Faith Cranor, and Norman Sadeh. 2011. Nudging users towards privacy on mobile devices. In *Proceedings of CHI 2011 Workshop on Persuasion, Nudge, Influence and Coercion*, Lincoln UK, July 2015. https://doi.org/10.1145/2783446.2783588.

Burruss, George, Christian Jordan Howell, Adam Bossler, and Thomas J. Holt. 2019. Self-perceptions of English and Welsh constables and sergeants preparedness for online crime. *Policing: An International Journal* 43 (1): 105-119.https://doi.org/10.1108/PIJPSM-08-2019-0142.

Brudy, Frederik, David Ledo, Saul Greenberg, and Andreas Butz. 2014. Is anyone looking? mitigating shoulder surfing on public displays through awareness and protection. In *Proceedings of The International Symposium on Pervasive Displays*, Copenhagen DK, June 2014. https://doi.org/10.1145/2611009.2611028.

Chen, Yan, and Fatemeh Mariam Zahedi. 2016. Individuals' Internet Security Perceptions and Behaviors: Polycontextual Contrasts Between the United States and China. *Mis Quarterly* 40 (1): 205-222. https://doi.org/10.25300/MISQ/2016/40.1.09.

Clarke, Ronald V. 1983. Situational crime prevention: Its theoretical basis and practical scope. *Crime and Justice* 4: 225-256. https://doi.org/10.1086/449090.

Clarke, Ronald V. 1995. Situational crime prevention. *Crime and Justice* 19: 91-150. https://doi.org/10.1086/449230.

Clarke, Ronald V. 1980. Situational crime prevention: Theory and practice. *The British Journal of Criminology* 20 (2): 136-147. https://doi.org/10.1093/oxfordjournals.bjc.a047153

Clarke, Ronald. 1997. *Situational crime prevention*. Guilderland, NY: Harrow and Heston Publishing.

Clarke, Ronald, and Ross Homel. 1997. A revised classification of situational crime prevention techniques. In *Crime Prevention at a Crossroads*, S.P. Lab, ed. Cincinnati, OH: Anderson Publishing. Retrieved from http://hdl.handle.net/10072/27163.

Cockerill, Aaron. 2015. Surprising new research: three-quarters of IT leaders have experienced a mobile data breach. *Lookout*, October 5. Retrieved from https://blog.lookout.com/mobile-data-breach-report.

Cohen, Lawrence E., and Marcus Felson. 1979. Social change and crime rate trends: A routine activity approach. *American sociological review* 44 (4): 588-608. https://doi.org/10.2307/2094589.

Conti, Mauro, Nicola Dragoni, and Viktor Lesyk. 2016. A survey of man in the middle attacks. *IEEE Communications Surveys & Tutorials* 18 (3): 2027-2051. https://doi.org/10.1109/COMST.2016.2548426.

Cukier, Michel. 2007. Study: Hackers Attack Every 39 Seconds. Retrieved from https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds.

Douglas, Stephen, and Brandon C. Welsh. 2020. Place managers for crime prevention: the theoretical and empirical status of a neglected situational crime prevention technique. *Crime Prevention and Community Safety*, 1-11. https://doi.org/10.1057/s41300-020-00089-4

Eiband, Malin, Mohamed Khamis, Emanuel Von Zezschwitz, Heinrich Hussmann, and Florian Alt. 2017. Understanding shoulder surfing in the wild: Stories from users and observers. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, Denver CO, May 2017. https://doi.org/10.1145/3025453.3025636.

Endsley, Mica R. 1995. Toward a theory of situation awareness in dynamic systems. *Human factors* 37 (1): 32-64. https://doi.org/10.1518/001872095779049543.

Fissel, Erica R. 2018. The reporting and help-seeking behaviors of cyberstalking victims. *Journal of interpersonal violence*, 0886260518801942. https://doi.org/10.1177%2F0886260518801942

Guerette, Rob T., and Shannon A. Santana. 2010. Explaining victim self-protective behavior effects on crime incident outcomes: A test of opportunity theory. *Crime & Delinquency* 56 (2): 198-226. https://doi.org/10.1177/0011128707311644.

Halpern, David. 2015. Nudging for good – David Halpern and Owain Service. Retrieved from https://www.bi.team/blogs/nudging-for-good-david-halpern-and-owain-service/

Herath, Tejaswini, and H. Raghav Rao. 2009. Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems* 18 (2): 106-125.

https://doi.org/10.1057/ejis.2009.6.

Holt, Thomas J., and Adam M. Bossler. 2014. An assessment of the current state of cybercrime scholarship. *Deviant Behavior*, 35 (1), 20-40. https://doi.org/10.1080/01639625.2013.822209

Howell, Christian J., David Maimon, John K. Cochran, Hattie M. Jones, and Ráchael A. Powers. 2017. System trespasser behavior after exposure to warning messages at a Chinese computer network: An examination. *International Journal of Cyber Criminology*, 11 (1), 63-77.

Honan, Brian. 2012. Visual Data Security White Paper. Retrieved from https://multimedia.3m.com/mws/media/950026O/secure-white-paper.pdf.

Jacques, Scott. 2019. Which source possesses the best data on the empirical aspects of criminal events? A theory of opportunity and necessary conditions. *Deviant Behavior* 40 (12): 1543-1552. https://doi.org/10.1080/01639625.2018.1559635.

Klasnja, Predrag, Sunny Consolvo, Jaeyeon Jung, Benjamin M. Greenstein, Louis LeGrand, Pauline Powledge, and David Wetherall. 2009. "When I am on Wi-Fi, I am fearless" privacy concerns & practices in eeryday Wi-Fi use. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, Boston MA, April 2009. https://doi.org/10.1145/1518701.1519004.

Klein, Gary. A. 1989. Recognition primed decisions. In *Advances in man-machine system research*, W. B. Rouse (Ed.). (Vol. 5, pp. 47–92). Greenwich, CT: JAI Press.

Krebs, Brian. 2012. FBI: Updates Over Public 'Net Access = Bad Idea. Retrieved from https://krebsonsecurity.com/2012/05/fbi-updates-over-public-net-access-bad-idea/

Maimon, David, Mariel Alper, Bertrand Sobesto, and Michel Cukier. 2014. Restrictive deterrent effects of a warning banner in an attacked computer system. *Criminology* 52 (1): 33-59. https://doi.org/10.1111/1745-9125.12028.

Madensen, Tamar D. 2007. "Bar management and crime: Toward a dynamic theory of place management and crime hotspots." Dissertation. Cincinnati, OH: University of Cincinnati

Marron, Donald. 2015. Obama's Nudge Brigade: White House Embraces Behavioral Sciences To Improve Government. Retrieved from https://www.forbes.com/sites/beltway/2015/09/16/obama-nudge-government/#745d3fbc2c99.

Newman, Graeme, and Ronald Clarke. 2003. *Superhighway robbery: preventing e-commerce crime*. Devon, UK: Willan Publishing. https://doi.org/10.4324/9781843924876.

Nobles, Matt R., Bradford W. Reyns, Kathleen A. Fox, and Bonnie S. Fisher. 2014. Protection against pursuit: A conceptual and empirical comparison of cyberstalking and stalking victimization among a national sample. *Justice Quarterly*, 31 (6), 986-1014. https://doi.org/10.1080/07418825.2012.723030

Norton. 2017. Norton WiFi Risk Report: Report of Online Survey Results in 15 Global Markets, Mountain View, California: Symantec. Retrieved from https://www.primo-europe.eu/wp-content/uploads/2017/07/2017-norton-wifi-risk-report-global-results-summary-en.pdf.

Raudenbush, Stephen W., and Anthony S. Bryk. 2002. *Hierarchical linear models: Applications and data analysis methods*, Vol. 1. Sage Publication.

Reyns, Bradford W. 2010. A situational crime prevention approach to cyberstalking victimization: Preventive tactics for Internet users and online place managers. *Crime Prevention and Community Safety* 12 (2): 99-118. https://doi.org/10.1057/cpcs.2009.22

Rouge, Phoebe. 2017. Researchers find bug in Wi-Fi network encryption. Retrieved from https://www.ftc.gov/tips-advice/business-center/privacy-and-security/data-security.

Rozee, Patricia D., and Mary P. Koss. 2001. Rape: A century of resistance. *Psychology of Women Quarterly* 25 (4): 295-311. https://doi.org/10.1111/1471-6402.00030

Sheridan, Lorraine P., and Tim Grant. 2007. Is cyberstalking different?. *Psychology, crime & law*, *13*(6), 627-640. https://doi.org/10.1080/10683160701340528

Smith, Kip, and Peter A. Hancock. 1995. Situation awareness is adaptive, externally directed consciousness. *Human factors* 37 (1): 137-148. https://doi.org/10.1518/001872095779049444

Ullman, Sarah E. 1997. Review and critique of empirical studies of rape avoidance. *Criminal Justice and Behavior* 24 (2): 177-204. https://doi.org/10.1177/0093854897024002003.

Ullman, Sarah E. 2007. A 10-year update of "review and critique of empirical studies of rape avoidance". *Criminal justice and behavior*, 34 (3), 411-429. https://doi.org/10.1177%2F0093854806297117

Watts, Steve. 2016. Secure authentication is the only solution for vulnerable public wifi. *Computer Fraud & Security* 2016 (1): 18-20. https://doi.org/10.1016/S1361-3723(16)30009-4

Welsh, Brandon C., Mark E. Mudge, and David P. Farrington. 2010. Reconceptualizing public area surveillance and crime prevention: Security guards, place managers and defensible space. *Security Journal* 23 (4): 299-319. https://doi.org/10.1057/sj.2008.22.

Worsley, Joanne D., Jacqueline M. Wheatcroft, Emma Short, and Rhiannon Corcoran. 2016. Victim's voices: Understanding the emotional impact of cyberstalking and individual's coping responses. *Sage*

open, 7 (2), 2158244017710292. https://doi.org/10.1177%2F2158244017710292

Wright, Ryan T., Matthew L. Jensen, Jason Bennett Thatcher, Michael Dinger, and Kent Marett. 2014. Research note—influence techniques in phishing attacks: an examination of vulnerability and resistance. *Information systems research* 25 (2): 385-400. https://doi.org/10.1287/isre.2014.0522

Wright, Ryan T., and Kent Marett. 2010. The influence of experiential and dispositional factors in phishing: An empirical investigation of the deceived. *Journal of Management Information Systems* 27 (1): 273-303. https://doi.org/10.2753/MIS0742-1222270111

Xiao, Bo, and Izak Benbasat. 2011. Product-related deception in e-commerce: a theoretical perspective. *Mis Quarterly* 35 (1): 169-196. https://doi.org/10.2307/23043494

Zafft, Andrew, and Emmanuel Agu. 2012. Malicious WiFi networks: A first look. In *37th Annual IEEE Conference on Local Computer Networks-Workshops*, Clearwater FL, October 2012. https://doi.org/10.1109/LCNW.2012.6424041

Ziegenhagen, Eduard A., and Dolores Brosnan. 1985. Victim responses to robbery and crime control policy. *Criminology* 23 (4): 675-695. https://doi.org/10.1111/j.1745-9125.1985.tb00369.x

Tables

Table 1. Descriptive Statistics (Study 1).

Variables	Mean	*SD*	Min	Max
Dependent variables:				
Uses Public Wi-Fi Network	0.23	0.42	0	1
Check Online Personal Accounts on Public Wi-Fi Network	0.43	0.49	0	1
Conceal Device Screen While Using Public Wi-Fi Network	0.88	0.31	0	1
Independent variables:				

Situational Awareness	3.28	1.12	1	5
Male	0.49	0.50	0	1
Age	19.60	1.90	17	39
Annual Income	1.31	1.43	1	12
Programing Experience	0.36	0.65	0	3
Note. n = 749				

Table 2. Public Wi-Fi Use and Adoption of Online and Offline Self-Protective Behaviors Regressed Over Individual's Situational Awareness (Study 1).

Variables	Uses Public Wi-Fi Network Model 1		Check Online Personal Accounts on Public Wi-Fi Network Model 2		Conceals Device Screen While Using Public Wi-Fi Network Model 3	
	b (*SE*)	OR	*b* (*SE*)	OR	*b* (*SE*)	OR
Situational Awareness	†0.13 (0.02)	1.14	†-0.12 (0.07)	0.88	**0.52 (0.11)	1.68
Male	*-0.44 (0.19)	0.64	0.21 (0.17)	1.23	0.01 (0.24)	1.01
Age	0.04 (0.04)	1.04	-0.05 (0.05)	0.95	-0.05 (0.05)	0.95
Annual Income	0.08 (0.05)	1.08	0.01 (0.05)	1.01	-0.04 (0.07)	0.95
Programing Experience	*-0.98 (0.52)	0.83	**-0.41 (0.15)	0.66	-0.11 (0.27)	0.89
Constant	2.77 (2.70)		1.02 (0.97)		1.51 (1.10)	
Pseudo R^2	0.03		0.02		0.05	

Ln likelihood	-378.17		-406.42		-253.99	
AIC	772.35		828.85		519.99	
Note. n = 749. b = regression coefficient; *SE* = standard error; OR = odds ratio; AIC = akaike information criterion. $^{\dagger}p \leq 0.10$, $^{*}p \leq 0.05$, $^{**}p \leq 0.01$.						

Table 3. Adoption of Online and Offline Self-Protective Behaviors Regressed Over Individual's Situational Awareness Among Public Wi-Fi Users Only (Study 1).

Variables	Check Online Personal Accounts on Public Wi-Fi Network Model 1		Conceals Device Screen While Using Public Wi-Fi Network Model 2	
	b (*SE*)	OR	*b* (*SE*)	OR
Situational Awareness	†-0.25 (0.15)	0.78	†0.52 (0.27)	1.69
Male	0.36 (0.37)	1.43	-0.82 (0.15)	0.44
Age	-0.17 (0.12)	0.84	-0.12 (0.12)	0.88
Annual Income	-0.41 (0.22)	0.65	-0.14 (0.12)	0.87
Programing Experience	-0.46 (0.33)	0.63	0.21 (0.49)	1.23
Constant	†4.35 (2.09)		3.74 (2.66)	
Pseudo R^2	0.07		0.09	
Ln likelihood	-107.14		-46.01	
AIC	226.28		104.02	
Note. n = 164. b = regression coefficient; *SE* = standard error; OR = odds ratio; AIC = akaike information criterion. $^{\dagger}p \leq 0.10$, $^{*}p \leq 0.05$, $^{**}p \leq 0.01$.				

Table 4. Descriptive Statistics (Study 2).

Variables	Mean	SD	Min	Max
Dependent Variables:				
Accessed Unknown Wi-Fi Network	0.16	0.37	0	1
% Devices Concealed	9.19	20.84	0	100
Independent Variables:				
% Employees	20.76	14.62	0	100
% Male	48.88	15.18	0	100
Morning	0.33	0.47	0	1
Afternoon	0.38	0.48	0	1
Evening	0.29	0.45	0	1
Other Network	0.80	0.40	0	1
Note. n = 208 (across 80 locations)				

Table 5. Logit and Linear Multilevel Random Intercept Models of Honeypot Sessions (Study 2).

Variables	Accessed Unknown Wi-Fi Network				% Devices Concealed	
	Model 1		Model 2		Model 3	Model 4
	b (*SE*)	OR	*b* (*SE*)	OR	*b* (*SE*)	*b* (*SE*)
% Employees	*-0.06 (0.02)	0.94	**-0.07 (0.03)	0.92	*0.28 (0.14)	*0.32 (0.14)

% Male			0.01 (0.02)	1.01		*0.20 (0.11)
Morning [a]			0.52 (0.56)	1.67		5.74 (3.11)
Afternoon [a]			0.30 (0.55)	1.34		2.10 (2.89)
Other Network			*-1.26 (0.64)	0.28		4.32 (5.19)
Constant	*-0.98 (0.52)		-0.65 (1.19)		4.52 (0.35)	-12.41 (0.82)
Rho	0.33		0.29		0.53	0.49
Df	3		7		4	8
Ln likelihood	-85.96		-83.26		-754.46	-750.22
AIC	177.93		180.53		1516.94	1516.44

Note. n = 208 (across 80 locations). *b* = regression coefficient; *SE* = standard error; OR = odds ratio; Rho = Spearman's Rho; Df = degrees of freedom; AIC = akaike information criterion. $^{\dagger}p \leq 0.10$, $^{*}p \leq 0.05$, $^{**}p \leq 0.01$. [a] Reference category = Evening

Figure

Figure 1. Observations Recorded During a One Hour Honeypot Session (Study 2).