Self-Protective Behaviors Over Public WiFi Networks

David Maimon, *University of Maryland*
Michael Becker, *University of Maryland*
Sushant Patil, *University of Maryland*
Jonathan Katz, *University of Maryland*

Abstract

The proliferation of public WiFi networks in small businesses, academic institutions, and municipalities allows users to access the Internet from various public locations. Unfortunately, the nature of these networks pose serious risks to users' security and privacy. As a result, public WiFi users are encouraged to adopt a range of self-protective behaviors to prevent their potential online victimization. This paper explores the prevalence of one such behavior---avoidance of sensitive websites---among public WiFi network users. Moreover, we investigate whether computer users' adoption of an online avoidance strategy depends on their level of uncertainty regarding the security practices of the WiFi network they login to. To answer these questions, we analyze data collected using two phases of field observations: (1) baseline assessment and (2) introduction of a private (honeypot) WiFi network. Phase one baseline data were collected using packet-sniffing of 24 public WiFi networks in the DC metropolitan area. Phase two data were obtained through introducing a honeypot WiFi network to 109 locations around the DC Metropolitan area and an implementation of a quasi-experimental one-group-post-test-only research design. Findings reveal that although most WiFi users avoid accessing banking websites using established public WiFi networks, they still use these networks to access social networks, email, and other websites that handle sensitive information. Nevertheless, when logged in to a WiFi network that has some uncertainty regarding the legitimacy and security practices of its operator, WiFi network users tend to avoid most websites that handle sensitive information.

1. Introduction

The expansion of public WiFi networks in small business (for instance coffee shops, restaurants), academic institutions, and municipalities in the USA and around the world [11,3] allows users to login to the Internet from various public locations and at all times of day. In most cases, these wireless networks are easily accessible to customers and other users, and do not require any form of user authentication or identification for using them [23]. Once logged in to these networks, public WiFi users tend to check their email accounts, access social networks, shop online, and even access their bank accounts [18]. Unfortunately, since many of the public WiFi networks are unencrypted [23] and allow for an easy distribution of malware [11], man-in-the-middle attacks [1], and hijacking connection [20], they pose series risks to their users' security and privacy.

Acknowledging these risks, the Federal Trade Commission (FTC) encourages public WiFi users to take specific precautions when using these networks. For instance, users are instructed to use encrypted WiFi networks, only enter personal identifying information on secured websites (i.e. websites that their URL address begins with https), use Virtual Private Network (VPN) connections, and avoid sending emails containing personal information (see https://www.consumer.ftc.gov). Few experts even go further to suggest that since malicious WiFi networks could be easily deployed by criminals in order to trick people to log into them [23], users should completely avoid online banking and accessing sensitive data when using a public WiFi network (even if these websites are encrypted). Unfortunately, despite the continued efforts that are being made to improve public WiFi users' awareness of these hazards and the security measures that they need to take [10], we still lack understanding of how common self-protective behaviors are among public WiFi users. Moreover, it is relatively unknown what could spark self-protective behaviors among internet users who employ WiFi hotspots.

Addressing these issues, this paper seeks to answer two key research questions; first, how established the self-protective practice of avoidance from accessing websites that handle sensitive information is among public WiFi network users? And second, does the uncertainty regarding the legitimacy of the WiFi network operator determine computer users' avoidance from accessing websites that handle sensitive information? To answer these questions, we analyze data collected using both survey and experimental research designs. The integration of two complimentary research designs allows a more thorough investigation of public WiFi users' online self-protective behaviors, as well as the context in which these behaviors are more likely to occur. We begin this paper with a brief overview of the important role of self- protective behaviors in preventing the completion of a criminal event, and situate this discussion in the context of the online environment and public WiFi users' decision-making process when accessing the network. We continue with a description of the survey methodology (phase 1) and the experimental research design (phase 2) we employed in our research. Followed by that we discuss findings from statistical analyses we performed. We conclude by considering the theoretical and policy implications of these findings.

2. Theoretical Framing

2.1 Victim Self-Protective Behaviors

Victim Self-Protective Behaviors (VSPB) occur when individual attempts to protect himself from becoming the victim of crime [2]. Broadly, criminologists differentiate between two major types of 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 a criminal event [21]. 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 [9]. Examples of behaviors that could be classified as non-forceful strategies include avoiding an offender, escaping, pleading and begging. Findings from past criminological research suggest that both forceful and non-forceful resistance can decrease the likelihood of sexual abuse and rape [15], domestic violence [2] and robbery [24,9] from occurring or escalating. These findings coincide with the theoretical rationale extended by two key criminological theories that aim to explain the probability of a successful criminal event to be completed: The Routine Activities Theory [5] and the Situational Crime Prevention perspective [4].

The Routine Activities Theory [5] focuses on identifying behaviors, activities and situational contexts that put would-be targets at risk for criminal victimization [19]. In their original formulation of the theory, Cohen and Felson suggested that the structure of aggregated daily routines determine the convergence in time and space of motivated offenders, suitable targets and capable guardians, and influence trends of predatory crime. For the purposes of this study, capable guardianship, or the presence of individuals capable of, and motivated to intervene on behalf of potential victims, is notably absent in the context of public WiFi. Reflecting on the relevance of VSPB in the context this theory, one may suggest that greater use of VSPB would complicate offenders' attempts to complete a criminal event and reduce its occurrence [9]. Moreover, victims' use of non-forceful resistance technique like evasion and avoidance will remove the victim from the criminogenic situation, and prevent the occurrence of a criminal event [24]. Simply put in the original context, the application of VSPBs should reduce the suitability of potential targets.

The Situational Crime Prevention perspective [4] is focused on the occurrence and development of criminal events. The underlying premise of this perspective is that criminals are rational, weighing the costs and benefits of their prospective behaviors, so successful crime prevention efforts must involve the design and manipulation of human environments to make offenders' decisions to get involved in crime less attractive [4]. Therefore, Clarke recommended the adoption of crime-specific prevention strategies (for instance, strategies targeting theft, robbery, burglary, vandalism, etc.) that fall into five categories: *increase offenders' effort, increase offenders' risks, reduce offenders' rewards, reduce provocations, and remove excuses* [7]. VSPB on its various forms are of utmost relevance in the context of this perspective since victim's resistance would increase offenders' effort to complete a criminal event and offset offenders' cost and benefit calculations [9].

Although past research has focused on the effect of VSPB on preventing offline victimization, we suspect that non-forceful resistance VSPBs are also relevant in preventing online victimization. For example, like installing a security or alarm system in someone's home to prevent burglary, installing antivirus software on one's computer is considered an effective practice for preventing malware attacks [16-17]. Similarly, while avoiding a potential neighborhood or street segment is proved to be an effective non-forceful strategy for reducing the probability of robbery [24], spending less time on untrusted or untrustworthy websites and downloading copyright protected material illegally to a computer may reduce individual likelihood to experience a wide range of cybercrimes [10]. Importantly, we believe that there is a need to differentiate between offline and online non-forceful VSPB in order to understand how these strategies reduce the probability of an online criminal event. For instance, [14] report that public WiFi users attempt to protect their privacy when working with the network by tilting or dimming their computer screens, as well as sitting with their computers angled toward the wall. These behaviors could be classified as offline non-forceful resistance strategies. In contrast, installing an antivirus package, using a secure VPN connection, and avoiding accessing and handling sensitive information while using public WiFi networks could be classified as an online non-forceful resistance strategies that reduce the probability of cybercrime from progressing.

2.2 The Current Research

Our focus in this paper is on internet users' online avoidance from accessing sensitive websites while using a public WiFi network. Specifically, we seek to determine *how common avoidance from accessing websites that handle sensitive information (banking, email, social networks and personal cloud – e.g. google drive, dropbox, etc.) among WiFi networks is*. Indeed, previous research has already investigated public WiFi users' online routines. For example, findings reported by the Identify Theft Resource Center [12] suggest that 57% of the public WiFi users they sampled logged into a work-related system like email or file sharing while using a public WiFi network and that 24% of respondents made purchase using a credit card while using the network. Similarly, [22] reports that 83% of public WiFi users use their emails, 68% use their social media accounts, 43% access work specific information, 42% shop online and 18% access banking websites while using public WiFi networks. While these reports are informative and suggest variation with respect to the type of websites that public WiFi users tend to access while employing public WiFi networks, these reports draw on problematic samples, employ questionnaires for gathering data from subjects, and fail to take into consideration the physical and temporal conditions which may influence public WiFi users' decisions to engage in these online behaviors. We suspect that a more hands on approach to assess public WiFi users' online routines with the network is to

see what people are actually doing on public WiFi network by monitoring locations which host a public WiFi hotspot and observing the traffic they generate.

In addition to exploring how likely public WiFi users are to avoid accessing websites that handle sensitive information, we also explore whether uncertainty regarding the owner of a WiFi network shapes users' avoidance from accessing websites that handle sensitive information. To this end, prior psychological theory and research indicates that decision makers tend to be ambiguity-averse [8,13]. Accordingly, when forming expectations about the consequence of their possible behaviors, individuals opt for prospects with known risks as opposed to unknown risks. In line with this rationale, we believe that the introduction of ambiguous information (i.e. missing information that prevents decision makers' ability to estimate the probability of an event) regarding a WiFi network and its operator, will disrupt public WiFi users' calculations of their risks of becoming the victims of cybercrime, and will induce more cautious online behaviors in contrast to when using a network whose owner is known.

3. Data and Methods

To answer these two research questions, we collected data across two phases: (1) a baseline assessment of user behavior on extant WiFi networks, and (2) an evaluation of if, and how individuals use an unknown network that was introduced. Phase one baseline data was collected by packet-sniffing extant public WiFi networks at 24 locations in the DC metropolitan area. In phase two, we introduced our own WiFi network in 109 locations around the DC Metropolitan area and implemented a quasi-experimental one-group-post-test-only research design. Like in phase one, for the second phase, we deployed private WiFi networks (honeypots) and packet-sniffed the internet traffic on these private networks.

3.1 Public WiFi Baseline Assessment

To explore public WiFi users' online behaviors we collected public WiFi network data by launching 72 packet sniffing sessions in 24 locations across Maryland and the DC metropolitan area using the software "Wireshark". Wireshark is a network protocol analyzer that can monitor and capture network packets that have not been addressed to the host. We used "Wireshark" to collect packet data in one hour sessions at three times of day (morning, noon and evening[1]), recorded the public WiFi speed, and counted the number of devices that used the network. Since in six of the sniffing session no computer users attend the location we report data from 66 sessions. These data from the public WiFi networks were used for identifying how computer users are using public wireless networks. Specifically, we examined unencrypted WiFi traffic to determine websites visited by users and the activities with which these websites are associated (e.g., checking email, watching videos, using a P2P file-sharing service, etc.), whether or not end-to-end encryption (e.g., SSL or a VPN) is being used, and whether malware is detected on the host and/or in the inspected traffic. Importantly, in order to protect people's privacy and maintain anonymity, the collected data was aggregated across each data collection session and not linked to specific users.

In addition to network data, we also collected data from the physical environment in which the public WiFi hotspot operated. Figure 1 presents an example of data collected from a location in Washington, DC during a 1-hour sniffing session by one of our research assistants. As may be observed in the figure, once arriving at a research location our research assistants diagrammed the physical layout of the space as well as recorded information about *the number of individuals who were present in each research site, number of male, number of female, number of customers, number of employees, number of observed smartphone devices, number of laptops, percent of individuals sharing a table, and percent of people sitting in adjacent tables.*

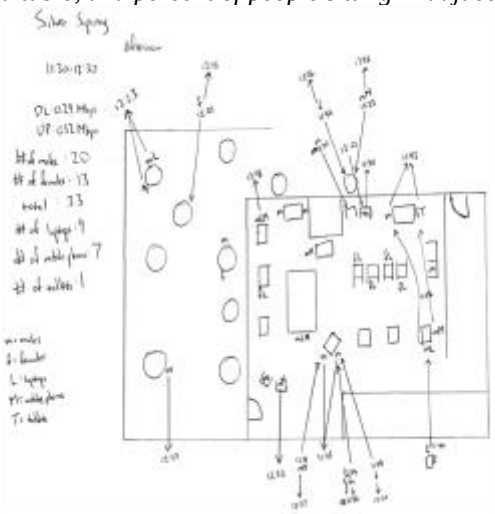

Figure 1. Observations Recorded During A One Hour Sniffing Session in Sliver Spring MD (Afternoon)

Finally, information regarding neighborhood demographic and social characteristics was downloaded from the U.S. Census website (available at www.census.gov). Specifically, we download neighborhood (census tract level) information regarding *the total population in the neighborhood, percentage of residents that are below the poverty line, percentage of residents in the community who are unemployed, percentage of households in the community that are headed by a female, percentage of residents living in the same house in the last 5 years, and percentage of foreign-born resident in the community.*

3.2 WiFi Network Honeypots

Next, to understand public WiFi users' behaviors on the network we also explored computer users' willingness to login to a WiFi network they were not familiar with (and which we owned). To do so, we introduced a new and unknown network to locations similar to those selected in phase one. In this experimental design, the characteristics and outcomes of interest were measured across both phases and thus can be compared on observable attributes.

[1] Morning sessions were defined as entirely within the hours of 8:00am and 11:00am, afternoon sessions were within the hours of 12:00pm and 2:00pm, and evening sessions were between the hours of 5:00pm and 8:00pm on weekdays.

Adopting this research design in our work, we selected 109 research sites with a wireless router of our own at three times of day (morning, noon and evening)[2] for each location. The router allowed users easy access to the Internet since it did not require login credentials (i.e. password and user names). Traffic on this network was closely monitored by a student who packet-sniffed our network using the "Wireshark" software and tools native to the router. Our goal in this was to determine the proportion of public WiFi users who are likely to roam around and look for WiFi networks to login to and use. We were also interested to understand these users' online behaviors while on the untrusted network. All in all, we observed and analyzed internet traffic on 34 of the 109 locations we visited (i.e. 31% of the research sites). Importantly, the current research does not seek to explain the variation between locations in which computer users accessed and did not access our networks. Instead the current work is focused on the type of traffic we observed on the WiFi networks we deployed. Thus, consistent with the data collected in the public WiFi baseline assessment phase, we collected information on online users' online behaviors and susceptibility to cybercrime victimization using "Wireshark". We also collected relevant information on the physical environment using observations. Finally, we downloaded information regarding neighborhood demographic and social characteristics from the U.S. Census website.

3.3 Ethical and Privacy Considerations

We have applied for an IRB approval for this project and the IRB team in the University of Maryland determined that our project does not involve human subjects, and hence does not require an IRB approval. Further, honeypot networks deployed in phase 2 of this study were clearly labeled as "private", and thus potential users knowingly trespassed on an unknown private network. In addition, we also consulted with the legal team at the University of Maryland and verified that the act of sniffing is legal in the state of Maryland. Indeed, the use of a free and public program to sniff in unsecure public networks has been ruled to be legal under the Wiretap Act (see "In re INNOVATIO IP VENTURES, LLC PATENT LITIGATION", District Court, ND Illinois 2012) and has been employed by [3] in their investigation of public WiFi networks in 20 international airports (located in 4 countries). However, in line with the University of Maryland Legal Team's recommendation, we did not initiate a sniffing session in public WiFi locations in which this activity was specifically prohibited by the network owner.

3.4 Dependent Variables

The data collected using Wireshark during our packet-sniffing sessions indicated that WiFi users employed the network for accessing wide range of websites. Indeed, we observed packet-data of advertisement, E-commerce, education, news, sport and video streaming websites. However, since our goal in this paper is focused on WiFi users' online self-protective behaviors, we observe in this work the relative number (i.e. proportion) of sniffing sessions and WiFi networks on which users accessed websites that handle sensitive information as a dependent measure. Specifically, we calculated the *proportion of packet sniffing sessions and WiFi network hotspots on which packet-data that is associated with banking, email, social network and personal cloud* websites was observed.

4. Results

4.1 How prevalent is avoidance from accessing sensitive websites among public WiFi network users?

We begin by presenting findings regarding the prevalence of packets originating from sensitive websites and observed over public WiFi locations. In the following, the unit of analysis is the location.[3] Figure 2 shows the proportion of sniffing sessions (N=66) at which banking, social network, email, and personal internet packets were observed. As indicated in the figure, banking websites packets were observed at 38% of the sniffing sessions we collected. In addition, packets originated in social network websites were observed at 86% of the sniffing sessions, packets from email accounts on 68% of the sniffing sessions, and packets from a personal cloud on 73% of the sniffing sessions.

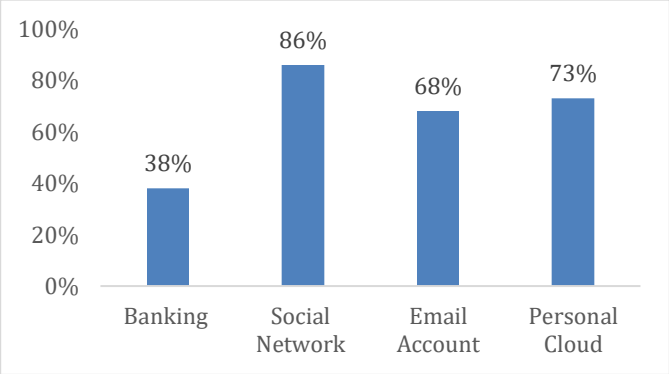

Figure 2. Internet Traffic Observed on Public WiFi Hotspots in the DC Metropolitan Area (N=24 Unique Locations).

Since we packet-sniffed the 24 locations during three times of day (morning, afternoon, and evening), we further explored whether the presence of packets from websites that handle sensitive information varies by time of day. Findings from this analysis are presented in Figure 3. As indicated in the figure, with few exceptions, the presence of packet data from banking, social network, email and personal cloud websites on public WiFi hotspot tended to be consistent throughout the day. Indeed, it appears that banking packets are less common during evening sniffing sessions than during morning and afternoon sessions, and that both email and personal cloud packets are less common on public WiFi hotspots during morning sniffing sessions than during afternoon and evening sessions. However, analyses from a chi-square test suggests that these differences are not statistically significant.

[2] With the same criteria as in phase one.

[3] These data were aggregated up from one to three hours of data collection sessions dependent upon the hours of operation for each location and most fairly represent the limitations of using DNS packet queries as an indicator of network traffic rather than presuming to measure the volume of said traffic.

These findings also suggest that public WiFi users generally do not avoid accessing websites that handle sensitive information. In fact, evidence from our packet-sniffing sessions suggests that public WiFi users access social media, email, and personal cloud accounts while using public WiFi hotspots. Still, the relatively low prevalence of locations where banking packets were observed indicates that public WiFi users may be taking steps to avoid accessing sensitive banking information from these networks.

4.2 Does Computer Users' Online Avoidance Depend on the Level of Uncertainty Regarding the WiFi Network?

Next, we explore whether ambiguity regarding the WiFi network and its owner determine users' probability of accessing sensitive websites. To answer this question, we compare the proportions of extant public WiFi hotspots on which banking, email, social media, and personal cloud website packets were observed with the proportions of honeypot WiFi networks on which similar packets were observed. Note that while the analyses performed to answer our first research question were focused on the presence of packet data on the *sniffing session (i.e each time we sniffed the network)*, we answer our second research question by investigating the presence of packet data on the *WiFi network (i.e. aggregating the three sniffing sessions we ran per each location l)*. Specifically, we employ the data collected during our initial phase of public WiFi network assessment (i.e. 24 locations) and compared it with packet data collected on our honeypot WiFi networks (i.e. 34 locations).

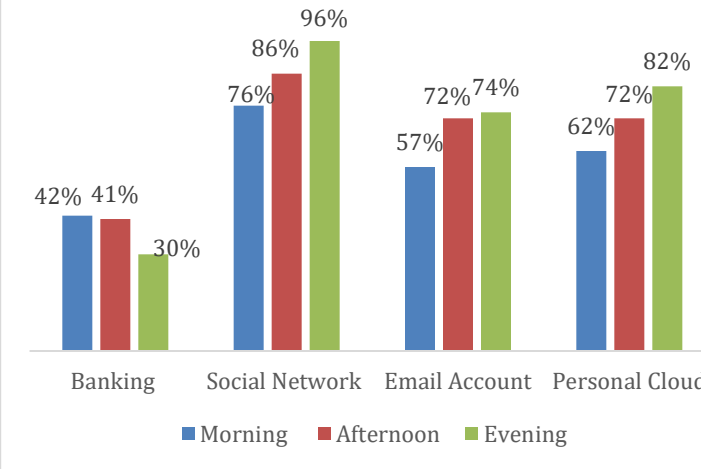

Figure 3. Internet Packets Observed During 66 Sniffing Sessions on Public WiFi Hotspots in the DC Metropolitan Area Across Three Times of Day

Before turning to answer our second research question, we first compare both the location and neighborhood level characteristics in which our research team either sniffed the public WiFi network, or deployed and observed traffic on the honeypot WiFi network that was deployed. These findings are presented in Table 1 and Table 2. As indicated in Tables 1 and 2, both the physical and social landscape and census tract characteristics of the locations we attended both in the assessment and honeypot phases of our project are very similar. In fact, the only significant difference between the contextual characteristics of the extant public WiFi hotspots and the contexts in which the honeypot WiFi networks were introduced was with respect to the number of mobile devices observed. Specifically, we observed a significantly higher number of mobile devices during the assessment of extant public WiFi network locations than in the locations where we deployed our own WiFi network. At the neighborhood level, it appears that the neighborhoods in which we deployed our WiFi networks had a significantly higher percentage of foreign-born residents than in the public locations with extant WiFi networks. Moreover, residential stability (i.e. percent living in the same house for more than 5 years) is significantly higher in the neighborhoods in which we surveyed the extant public WiFi networks than in the neighborhoods where we deployed our honeypot network.

Location Physical and Social Characteristics	**Extant Public WiFi Network**	**Honeypot WiFi Network**
	Mean (SD)	**Mean (SD)**
Number of people	23.47 (12.30)	21.16 (17.39)
Number of males	11.25 (5.75)	10.66 (9.75)
Number of females	10.97 (6.18)	10.50 (8.42)
Number of customers	20.93 (11.49)	18.66 (16.39)
Number of employees	2.53 (1.69)	2.49 (2.14)
Number of mobile devices (observed)	8.22 (6.64)	2.77* (3.13)
Number of Laptops (observed)	4.31 (5.03)	2.70 (6.05)
% people sharing a table	61.88 (23.94)	69.77 (43.23)
% people sitting in adjacent tables	74.16 (25.98)	77.16 (56.85)

* $p<0.05$ ** $p<0.01$

Table 1. Location Physical and Social Characteristics of Public WiFi Hotspots and Locations in which WiFi Networks Were Deployed

Next to investigation of significant differences between the physical and social landscapes and neighborhood characteristics across networks, we also test for significant differences between the presence of traffic to websites that do not require accessing sensitive information on the two types of networks. Findings from that analysis are reported in Table 3. As shown in Table 3, users of both extant public WiFi networks and the honeypot WiFi networks used the Internet for accessing educational, news, sport and video streaming websites. Moreover, packets reflecting advertisement traffic were observed on both type of networks. However, the proportion of

extant public WiFi hotspot locations with packets in these five website types is significantly higher than the proportion of honeypot WiFi network locations with the same type of packets.

Finally, to answer our second question we compared the proportion of extant public WiFi locations and locations where our own WiFi networks were deployed on user access to websites that handle sensitive information. Findings from this analysis are presented in Figure 4. As indicated in the figure, banking website packets were observed on 54% of the extant public WiFi hotspots that we surveyed. In addition, packets indicative of social network website use were observed on 100% of the extant public WiFi hotspots, packets from email sites on 83% of the hotspots, and packets from a personal cloud on 87.50% of the public WiFi hotspots. In contrast, no banking, email or personal cloud packets were observed on the honeypot WiFi networks. However, in close to 68% of the locations with WiFi networks we deployed we observed packets indicative of social media website use. To test whether the proportion of extent public WiFi locations and locations where our own WiFi networks differ on the presence of packets of websites that handle sensitive information we ran a T-test for determining whether the difference between the two proportions is significant. Findings from these t-tests reveal statistically significant difference between public WiFi and honeypot WiFi for each type of packet that is originated in website that handle sensitive information. Thus, this finding suggests that internet users are more likely to avoid accessing websites that transmit sensitive data when employing WiFi networks that carry uncertainty with respect to their owners.

Neighborhood Characteristics	**Public WiFi**	**Unfamiliar WiFi Network**
	Mean (SD)	**Mean (SD)**
Total population	3405 (1384.24)	4213 (2781.90)
Percent poverty	14.97 (9.09)	13.92 (13.26)
Percent unemployed	5.70 (4.00)	4.43 (3.10)
Percent foreign born	13.62 (10.42)	21.34* (14.46)
Percent female headed household	25.18 (18.03)	35.11 (61.17)
Percent living in the same house for more than 5 years	77.86 (9.40)	70.06** (11.07)

* p<0.05 ** p<0.01

Table 2. Census Tract Characteristics of Extant Public WiFi Hotspots and Honeypot WiFi Deployment Locations

5. Discussion

As public WiFi use proliferates and the number and speed of hotspots continues to grow, the commensurate risk of cybercrime on these networks is likely to rise accordingly. Drawing on the VSPB perspective, we designed and collected two phases of data to assess first how individuals make use of known, albeit often unsecured, wireless networks, and second, if, and how individuals would utilize an unknown network of uncertain management and origin. First, we asked how established the VSPB of avoidance is on websites that handle sensitive information among WiFi network users. Second, we sought to consider if uncertainty regarding the provenance of the WiFi network is associated with differential adoption of this avoidance technique. Findings from our unique field study provide several insights. First, we find some support for the extension of the VSPB framework to cyber environments. Insofar as self-protective behaviors may be concerned in the physical world, it appears that when connected to a public WiFi network, in more than half of the locations that we observed, individuals did not access banking websites. This finding was somewhat attenuated when considering the traffic to Social Networks, Email, and Personal Cloud services. This suggests that while there may be a salient risk associated with accessing ones bank on public WiFi, either due to the ubiquity of, or ambivalence toward disclosure of potentially less sensitive details available on social media, in emails, and backed up on personal cloud services, this traffic may not be conceived of as concerning to users.

Packets type	**Proportion of extant Public WiFi Locations with Packets Observed (n=24)**	**Proportion of honeypot WiFi Locations with Packets Observed (n=31)**
Advertisement	.83	.65**
Education	.41	.21**
News	.70	.27**
Sport	.41	.09**
Video streaming	.67	.23**

* p<0.05 ** p<0.01

Table 3. Proportion of Extant Public WiFi and Honeypot WiFi Network Locations in the DC Metropolitan Area with Different Types of Packets

Second, we find support for the notion that the introduction of uncertainty to the source and management of WiFi networks (as on our honeypots) could serve as a deterrent for sensitive web traffic by users. Consistent with [8] and [13], individuals who chose to login to honeypot networks appeared to be more cautious in their sensitive web traffic, only accessing social media in addition to less vulnerable sites. Again, the evidence of social media traffic suggests that the inter-connected world that we live in may habituate individuals to sharing such details as are present on their public social media profiles. However,

this is not to say that such ambivalence to disclosing these details is without risk. As can be seen from cases of cyber-stalking and cyber-bullying, access to an individual's social media account can be a very damaging in the wrong hands. In sum, the application of avoidance as a VSPB online, when incorporated with the use of appropriate antivirus software and safe internet behavior when on unsecured networks retains an important role in limiting victimization risk on public WiFi.

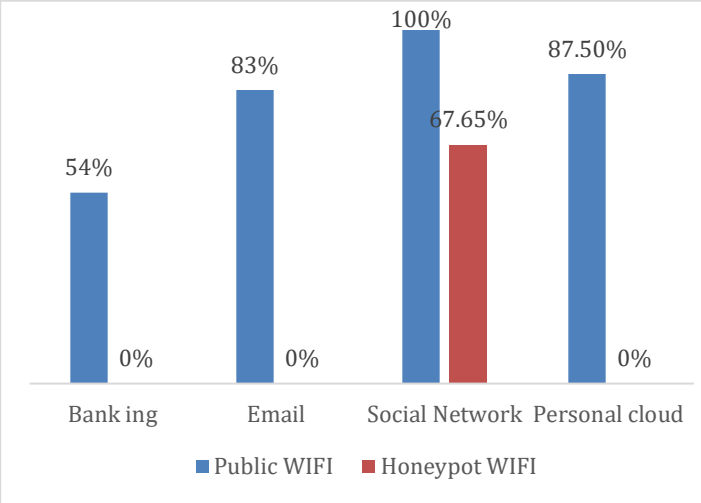

Figure 4. Internet Packets Observed on 24 Public WiFi Location and 34 Honeypot WiFi Networks

Finally, it behooves us to account for the limitations of this project. Due to the abundance of public WiFi networks, establishing a sampling frame from which to draw a representative sample of locations or networks was beyond the scope of this project. Thus, the findings presented herein are descriptive in nature and should be qualified as such. Future research should consider a means from which to obtain a census of specific types of WiFi hotspots from which to draw a more generalizable sample. Furthermore, additional characteristics of WiFi traffic and network users should be considered and controlled for in future analyses, including the base rate of traffic to given types of websites, the number of devices on networks, and duration of device network use. Additionally, while the use of Wireshark for categorizing DNS packet queries to servers represents an important first step in assessing network traffic on extant public and honeypot WiFi networks, future research should consider the use of HTTP and HTTPS packets for greater granularity of traffic data.

6. Conclusions

Avoidance from accessing websites that handle sensitive information is a type of online self-protective behavior that could be easily employed by public WiFi users to prevent their potential cybercrime victimization. While this avoidance strategy is rare among public WiFi users' in the context of social media, email, and personal cloud services, it appears to be quite common with respect to banking websites. Moreover, increasing the level of uncertainty regarding the WiFi network's legal owner and operator is associated with an increased likelihood of avoiding websites that handle sensitive information.[4]

References

[1] Aime, M. D., Calandriello, G., & Lioy, A. 2007. Dependability in wireless networks: Can we rely on WiFi?. *IEEE Security & Privacy*, *5*(1).

[2] Bachman, R., Saltzman, L. E., Thompson, M. P., & Carmody, D. C. 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.

[3] Cheng, N. , Xinlei W, Wei C., Prasant M. and Aruna S. 2013. "Characterizing Privacy Leakage of Public WiFi Networks for Users on Travel." Proceeding of INFOCOM'13 IEEE.

[4] Clarke, R V. 1995. Situational crime prevention. *Crime and justice* 19: 91-150.

[5] Cohen, L.E. and Felson, M. 1979. Social Change and Crime Rate Trends: A Routine Activity Approach. American Sociological Review 44: 588-608.

[6] Consolvo, S., Jung, J., Greenstein, B., Powledge, P., Maganis, G., & Avrahami, D. 2010, September. The Wi-Fi privacy ticker: improving awareness & control of personal information exposure on Wi-Fi. In *Proceedings of the 12th ACM international conference on Ubiquitous computing* (pp. 321-330). ACM.

[7] Cornish, D. B., & Clarke, R. V. 2003. Opportunities, precipitators and criminal decisions: A reply to Wortley's critique of situational crime prevention. *Crime Prevention Studies, 16*, 41-96.

[8] Ellsberg, D. 1961. Risk, ambiguity, and the Savage axioms. *The quarterly journal of economics*, 643-669.

[9] Guerette, R. T., & Santana, S. A. 2010. Explaining victim self-protective behavior effects on crime incident outcomes: A test of opportunity theory. *Crime & Delinquency*, *56*(2), 198-226.

[10] Holt, T. J., & Bossler, A. M. 2014. An assessment of the current state of cybercrime scholarship. *Deviant Behavior*, *35*(1), 20-40.

[4] We would like to thank our reviewers for their thoughtful comments in improving the clarity of this and future work.

[11] Hu, H., Myers, S. Colizza V., &Vespignani, A. 2009. "WiFi Networks and Malware Epidemiology." PNAS 106(5): 1318-1323.

[12] Identity Theft Research Center. 2012. Public WiFi Usage Survey. Available at: https://www.idtheftcenter.org/images/surveys_studies/PublicWiFiUsageSurvey.pdf

[13] Kahneman, D., & Tversky, A. 1979. Prospect theory: An analysis of decision under risk. *Econometrica: Journal of the econometric society*, 263-291.

[14] Klasnja, P., Consolvo, S., Jung, J., Greenstein, B. M., LeGrand, L., Powledge, P., & Wetherall, D. 2009, April. 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* (pp. 1993-2002). ACM.

[15] Kleck, G., & Sayles, S. 1990. Rape and resistance. Social Problems, 37(2), 149-162.

[16] Lalonde Lévesque, F., Nsiempba, J., Fernandez, J. M., Chiasson, S., & Somayaji, A. 2013. A clinical study of risk factors related to malware infections. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security* (pp. 97-108). ACM.

[17] Lalonde Lévesque, F. L., Fernandez, J. M., & Somayaji, A. 2014. Risk prediction of malware victimization based on user behavior. In *Malicious and Unwanted Software: The Americas (MALWARE), 2014 9th International Conference on* (pp. 128-134). IEEE.

[18] Norton. 2013. 2013 Norton Report. Symantec

[19] Pratt, T.C., Holtfreter, K. & Reisig, M.D. 2010. Routine Online Activity and Internet Fraud Targeting: Extending the Generality of Routine Activity Theory. Journal of Research in Crime and Delinquency 47: 267-296.

[20] Song,, Y., Yang C., & Gu, G. 2010. Who is Peeping at Your Password at Starbucks? – To Catch an Evil Twin Access Point. In: Proc. 2010 IEEE/ IFIP International Conference on Dependable Systems and Networks (DSN).

[21] Ullman, S. E. 1997. Review and critique of empirical studies of rape avoidance. Criminal Justice and Behavior, 24(2), 177-204.

[22] Xirrus. 2016. Rolling the Dice with Public WiFi. Available at: https://www.xirrus.com/pdf/Rolling-The-Dice-With-Public-WiFi.pdf

[23] Zafft A. & Ago E. 2012. "Malicious WiFi Networks: A First Look." 7th IEEE Workshop on Security in Communication Networks.

[24] Ziegenhagen, E. A., & Brosnan, D. 1985. Victim responses to robbery and crime control policy. Criminology, 23, 675-695.