THE ROLE OF TRUST AND OPTIMISTIC BIAS IN PUBLIC WI-FI SOCIAL ENGINEERING

By

SAMANNTHA KRISTAN WOOD

_____

A Thesis Submitted to the Honors College

In Partial Fulfillment of the Bachelors degree
With Honors in

Management Information Systems

THE UNIVERSITY OF ARIZONA

MAY 2016

Approved by:

_____

Dr. Matthew J. Hashim
Department of MIS

Abstract

What is social engineering? What is a malicious hotspot? What does being a victim of a social engineering attack mean? Perhaps most importantly, what about the human mind helps make social engineering so successful? These are the main questions I address in this paper. I begin by defining social engineering and providing an overview of its nature and why it is a problem, discussing studies and papers written on the topic. I argue that there are two underlying vulnerabilities that allow so many people to be the targets of social engineering attacks: trust and the optimistic bias. Drawing from theories about online trust and interpersonal trust, I analyze how four components of trust affect how and why people connect to public Wi-Fi connections. I also consider the role of the optimistic bias in why users continue to access sensitive information on public hotspots. To get a better understanding of these theories in action, participants have been surveyed on their knowledge of risks associated with connecting to unknown Wi-Fi and their usual behaviors on their devices.

The Role of Trust and Optimistic Bias in Public Wi-Fi Social Engineering

Introduction

As most services are establishing an important presence online, people are finding ways to exploit or steal the information surging from device to device. Trust has been noted as a key factor of website success. A well-done and maintained webpage can be the difference between making and losing a sale. But, looking deeper than the webpage, how much trust is needed for a user to connect to a Wi-Fi hotspot?

Consider this hypothetical situation. You enter an arena to see your favorite sports team. As you wait for the game to start, you think about an upcoming trip you plan to take. The Internet connection is not strong, so you check the Wi-Fi connections available. You see an open "ArenaWiFi," and select it. You proceed to check message boards of where you're going, book a night's stay in a hotel, and purchase the flights. You then remember you need to buy a gift for your nephew's birthday coming up. You take advantage of the remaining time before the game to go on the Internet to order something a kid might like. With the entering of your name and credit card number, your order is confirmed before the game starts.

Two weeks later, you get a call from your bank while on that vacation you booked. Your bank reports some suspicious charges on your credit card. When you get home, you find that your back window was shattered and someone had broken into your home. How could this have happened? You were a victim of a social engineering attack.

What went wrong here? Well, it started with connecting to a malicious hotspot. Social engineering is an attack on a person's innate vulnerability to trust in order for the attacker to obtain information. While few people are aware of this phenomenon, all are at risk. Social engineering attacks can be online or off-line. I will focus on the online dimension of it. More

specifically, I will focus on how social engineers—or social hackers—can use malicious public hotspots to launch a series of attacks on unknowing device users. A malicious hotspot is one that has either been infected or set up by an attacker. The danger with this is that the only way a user can determine if the hotspot is legitimate is by the name of the hotspot, and whether or not it requires a passcode.

A significant amount of trust is placed on the validity of the hotspot each time someone connects to it. But is that the only factor that induces a user to choose public Wi-Fi? With so many people using public Wi-Fi, is it possible that all of them are capable of trust enough to continue connecting? What if some people are naturally distrusting? Do they avoid usage of public networks entirely?

In addition to trust, I want to argue that there is a second factor at play: the optimistic bias. This heuristic assures users that despite possible consequences, bad things will not happen to them. It differentiates between *others* and *you*, creating a more optimistic situation for the self. Bad things are more likely to happen to *others* than they are to *you*. This is an extremely common psychological assumption that plays a significant part in why people take varying degrees of risk every day. Like the name suggests, it compels the user to be optimistic about the outcomes. Together, trust and the optimistic bias can be a powerful driver in a user's decision to connect to a public network.

The fact is, connecting to unsecure Wi-Fi means risking the loss of critical information that can lead to adverse effects. While there are many aspects of trust that could contribute to why people connect to the hotspots that they do, I will focus on four: the perception of credibility in the name, knowledge of associated risks, physical location of the user, and ease of access. I

will then explain why trust is not sufficient in itself; why the optimistic bias is needed to cover all the bases.

Am I at Risk?

How exactly did your credit card number get stolen while you were at the sports game? The first mistake was connecting to the malicious hotspot; but the second mistake was entering your credit card number while connected to that hotspot. (Holding your credit card up to read it in the middle of a crowded area where the seats are angled for the purpose of *seeing over your shoulder* is a mistake here, too, but I will not go into that for the purposes of this paper.)

Keep in mind that not all social engineering attacks lead to a result as consequential as the example above. That would be a somewhat rare case. Social engineering can go undetected and is not always as deleterious as that. However, it certainly can be and it is important to understand that.

Entering credit card information while connected to a malicious hotspot sets the stage for third-party interception. The social engineer that set up that hotspot was waiting for this moment. Many websites do not encrypt the information that you enter, letting it travel through the web like an open book to hackers. Without encryption, someone would have no problem stealing that credit card number you just entered to buy your nephew a gift.

There are websites and applications that encrypt your data. Banks, many brand name sites, and most websites that require you to login to use them will indicate with a little lock icon next to the web address that the website is secure. These websites will encrypt the data you enter, which can still be read with more effort on the hacker's end. Chances are if you connect to a malicious hotspot and search "Tickets for XYZ," the hacker will anticipate that you are about to

make a purchase. Although he cannot get your credit card information as directly on an encrypted site, he may also be prepared to put in the extra effort to try and crack the code.

"The chances of you being hacked far exceeds the chances of your home being burglarized. This is a big business." Kevin Clark, a first assistant Monmouth County prosecutor, warns that anyone using public Wi-Fi should understand that anything they do online is visible to strangers (Higgs, 2013, *USA Today*). Convenience too often exceeds precaution. It only takes seconds for information to be intercepted by a third-party and captured on another computer. For this reason, unsecure Wi-Fi is never a good idea.

Yes, you are at risk.

The Perception of Credibility in the Name

Many may think that malicious hotspots can be spotted a mile away. Contrary to that belief, connections do not usually read: hackerz_wifi or ConnectToGetHacked. They are often disguised as something many would consider legitimate.

The list of connections available at the local airport can look a lot like this:

Free PHX Boingo WiFi

PHX_SKY_HARBOR

Phoenix_Airport

airportwifi

SkyHarborHotspot

Trents_Wifi

Free_Wifi

Which one is legitimate? The perception of credibility is the factor that drives users to choose PHX_SKY_HARBOR over airportwifi. It is also, however, the factor that drives people

to select SkyHarborHotspot over Free PHX Boingo WiFi. The latter is the legitimate Wi-Fi service provided by Phoenix Sky Harbor courtesy of Boingo Wireless.

The factors that go into the perception of credibility include trigger words, spelling, capitalization, and punctuation. Errors in spelling, punctuation, and grammar are enough to reduce credibility in any situation whether it be in a report or a hotspot name. The way combinations of words are perceived are generally the same among the public; however, it is also likely that someone might perceive PHX_SKY_HARBOR more credible than Phoenix_Airport simply because of the capitalization utilized in the name.

Credibility leads to a feeling of trustworthiness. Corritore, Kracher, and Wiedenbeck (2003) defined online trust as "an attitude of confident expectation in an online situation of risk that one's vulnerabilities will not be exploited," (p. 740). They also note that credibility is a trigger for trustworthiness (p. 748). Furthermore, when users connect to Wi-Fi that appears credible, they trust that nothing bad will occur. To a user, a high perception of credibility equates to a low perception of risk. A low perception of risk leads to a higher degree of trust.

This factor is something that I will test in a later experiment where I set up access points and alter the name of the networks to see how many people connect. I select a few locations on the campus of the University of Arizona and its surrounding Tucson area to conduct this experiment. The variable in this case is the network names, which I will alter in terms of spelling, capitalization, punctuation, and trigger words. By trigger words I mean using a nearby landmark—such as Coffee Shop XYZ—in the name of the network or including the word "free." The use of trigger words improves the perception of convenience, which may be a factor in determining credibility. This is why "SkyHarborHotspot" may be perceived as more credible than "airportwifi."

Knowledge of Associated Risks

Kevin Mitnick defined social engineering as the art behind getting someone to do something that they would not normally do for a stranger (2002, p. 7). It is, essentially, capitalizing on a person's lack of knowledge or awareness. The use of deception and manipulation to gain information is not a new trend. In fact, you might encounter it daily.

Consider, for example, something more arbitrary than a credit card number or customer information. Instead, consider grade school. You spent all night watching re-runs of your favorite TV show and forgot you had a math assignment due the next day. When first period comes along and you realize you have not completed the assignment, and will receive that dreaded F, you decide that you need to get the answers from someone. This becomes your target information. You locate the girl who always gets A's in the front row of the class. She has the information. She becomes your target.

The smart girl in the front row does not know how you spent the previous night. You can use that lack of knowledge to your advantage. You make sure you walk in front of her after class and theatrically muster up your most believable sobbing sound. She asks what the matter is, and you tell her that your dog ran away last night. You spent so long wandering the neighborhood looking for him, that you did not get a chance to work on the math assignment. The girl takes pity on you and offers her help to finish the assignment. You gratefully accept and play the guessing game until she shows you exactly how to do the problems. You have successfully used manipulation to acquire information. Moreover, the girl is none the wiser. This is an arbitrary example of social engineering.

Would that girl have offered information to the boy if she were aware that he watched television all night? Or that did not even have a dog? No, probably not.

Would she have expected someone to directly ask for her answers? Probably. Was she expecting someone to deceive her and indirectly ask for her answers? Evidently not.

The knowledge of associated risks when it comes to social engineering is a key aspect in the exploitation of data. Mitnick alongside most researchers of social engineering and information security deem humans the weakest link. They call this the human factor. Humans are subject to naivety, gullibility, obliviousness, unawareness, or plain ignorance. Well-known early anarchist Emma Goldman said, “The most violent element in society is ignorance.” This saying rings true with social engineering as ignorance is often the source of information security’s demise.

Returning to the idea of a malicious hotspot, it is common that users do not often know what they signing up for when they connect to unsecure Wi-Fi. For example, it would be simple for someone to think that the Wi-Fi made available in their apartment complex by the management staff is safe to use. It may be. However, who are the other few hundred users of the same Wi-Fi connection? Do you know all of them? Do you know what their intentions are? Computers are quick to alert us when we connect to such networks. “This connection is unsecure. Your activity may be monitored.” These messages are overlooked a majority of the time. If the access point is managed by the apartment’s staff, then it *must* be safe.

People who think this way are too many. It displays a lack of knowledge of the associated risks, which include interception of information such as your name, address, credit card number, account information, and the list goes on.

Being wary of public Wi-Fi is a much safer habit than trusting your local coffee shop, a brand name department store, a fancy restaurant, or even your library. It is beneficial to remember that while there is software that can protect your computer, there is also software that

can break it down. Hacking software is available, and it poses a threat especially to anyone who uses public Wi-Fi and makes it that much easier for attackers. How many walls would you want around your castle? Connecting to public Wi-Fi takes down a pretty thick one.

As historian Daniel J. Boorstin said, “The greatest obstacle to discovery is not ignorance—it is the illusion of knowledge.” Users often think that the minimal antivirus software can protect them from the theft of information. That is untrue. Mitnick uses an example in his book, *The Art of Deception* (2002), which relates the illusion of safety to a homeowner that spends a good amount of money on the toughest of tumbler locks for his front door. The lock is pickproof, so his home should be safe. However, the home has windows. It also has a garage. Both provide other entry points to an attacker. The expensive lock is not enough to keep out all of the intruders. The lock is just an illusion of safety to the homeowner, just as standard protection software is.

Security of information is more often a human problem than anything else. Lack of knowledge of the risks associated with hotspot connections is more than likely responsible for most security breaches involving information theft. This is why a solid knowledge of the risks associated with malicious hotspots and social engineering is a key component to preventing attacks. Everyone should be educated on the dangers of social engineering no matter their frequency of internet use or age. Unfortunately, the concept is not given the attention it deserves.

Physical Location of the User

The physical location where the user is accesses a network plays a huge part in whether or not they deem it safe enough to connect to Wi-Fi. For example, someone sitting in a library is probably much more likely to connect to an available access point as opposed to someone sitting at a gas station off the highway in Newark, New Jersey. If you find it appropriate to ask yourself,

"Why would there be Wi-Fi here?", then you should be safe to assume that the Wi-Fi is not safe to use.

Additionally, users in any public place should be wary of the Wi-Fi connections that they can access for free and without a passcode. Public places are the targets for social engineers using malicious hotspots. Coffee shops, restaurants, theatres, arenas, airports, etc. are all feeding grounds for thieves looking to steal private information. The more people, the higher the traffic for malicious hotspots. People are tricked by the convenience of the open Wi-Fi connections. Furthermore, with the onslaught of available connections, people expect to have Wi-Fi installed almost anywhere. Most do not consider the safety of it.

Cities have begun to install Wi-Fi in parks for the convenience of visitors. While this is being done with good intentions, it also opens the door for social engineers to prey on those looking to connect. Harkening back on the perception of credibility in the name, social engineers might try to trick users by taking the city-hosted hotspot's name and tweaking it. Brookyn_WiFi looks a lot like Brooklyn_WiFi to the tourist eager to post a picture to Instagram.

Hotels are interesting places in terms of Wi-Fi. Consider the hotel that offers free Wi-Fi and requires you to enter your room number and last name to confirm that you are a registered guest in the system. That seems secure. However, connection to the hotel's Wi-Fi is open to all of the hotel's guests. Connecting to it means that you are willing to trust that none of the other hotel guests are hackers or social engineers looking to acquire your information. The Wi-Fi, therefore, is not as safe as guests might think. For the purposes of travel, use of a VPN (virtual private network) is highly recommended to protect your information.

A very common place for dozens of access points is the airport. It is often hard to tell which networks are legitimate and which are not verified. If this is the case, you should ask a

staff member of the airport which is the verified connection. Do not make the mistake of thinking just because the airport hosts a Wi-Fi connection that the connection is secure and your information is safe. Again, everyone who connects to that Wi-Fi is theoretically able to monitor your activity. Do not be fooled by the convenience of airport Wi-Fi.

For the purposes of my data collection, I will focus on high-traffic areas where the campus-wide UAWiFi does not reach. This will prompt users to seek a different WiFi connection. These places are just beyond the campus in the surrounding areas including local coffee shops and restaurants. Of course, the goal of this experiment is not to steal any information from users, but to record the number of users that simply connect to the access point that I set up. Connecting to my access point will direct users to a survey to assess their knowledge of social engineering and to understand their typical behaviors when using the internet in a public area.

Ease of Access

Convenience is a key reason why users throw caution to the wind and connect to any access point available to them. “Is there Wi-Fi?” has become a common question in most public places such as restaurants and cafes, especially among young adults. Setting up and configuring a Wi-Fi router is a task that can be done by almost anyone. Routers can be purchased for relatively low prices, making it accessible to many people. The installer has the opportunity to name and alter the settings for the hotspot.

For the purposes of this paper, I will discuss the factor of ease of access in terms of the user. The convenience of Wi-Fi is the primary reason that users connect to it. Rather than use their 3G/4G/LTE network on their mobile phones, Wi-Fi provides a less costly and faster option. Moreover, many users opt not to set up a VPN (Virtual Private Network) if they do not spend a

great amount of regular time on public Wi-Fi. This is a mistake because it leaves your actions exposed.

Using you mobile phone as a hotspot for your laptop would be a safer option than connecting to public Wi-Fi, but it may actually be more expensive than the monthly fee to set up a VPN. This is due to the extensive amount of data phone-activated hotspots can consume. Either option poses an extra level of action on the end of the user, which the convenience of public Wi-Fi overrides.

Literature Review

Leakage of Data

Encryption techniques have not been greatly utilized among public access points. WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access), and WPA2 (Wi-Fi Protected Access II) are all available for 802.11 wireless networks. This is because users of public Wi-Fi require more open access for quick connections. Users of public Wi-Fi are typically in passing and only need to use it to complete a few tasks, so setting up security measures may deter users from connecting at all.

The information that can be leaked includes device names, email addresses, network names, MAC addresses, and network providers (Cheng et al., 2013, p. 2771). How can someone get this information?

Your device has a name. It could be “Greg’s iPhone” or “Shelley’s Android” or some other identifier. In searching for an access point, the device sends out a domain name query via multicast. The query would contain the name of the device as well as the IP address. Already, this exposes the connection between the user’s name and their activities. Anyone within communication range can see the device name due to multicast DNS.

Furthermore, information can be leaked from webpages due to communication traffic. Searches online can reveal nationality, frequented stores, even banks that the user comes in contact with. If you consider browsing to be a conversation that you have with your device, you will be able to understand the concept of eavesdropping. Packets can be eavesdropped on. Recommended pages come from advertisers that have gotten ahold of your previous searches, revealing your interests. Their recommendations can be exposed to the social engineer behind the public Wi-Fi connection. Browsing history can reveal a lot about the user, which can set them up for a social engineering attack.

In "Characterizing Privacy Leakage of Public WiFi Networks for Users on Travel" (2013), Cheng et al. stated, "By looking at the content of the packets sent from the advertisers, it is possible to infer users' private information based on profiled advertisements," (p. 2771). Users can tell by the advertisements that appear in the sidebar, popups, or even within the content itself that their activity has been tracked by marketers. This makes the ads relevant and meaningful rather than annoying and unrelated to your interests. These are called user-tailored advertisements. While they have succeeded in boosting sales, they have also succeeded in leaking privacy.

The table below summarizes findings from the paper, "Characterizing Privacy Leakage of Public WiFi Networks for Users on Travel," researched by Cheng et al. of the University of California-Davis who analyzed datasets from 20 different airports in 4 countries (p. 2772).

Type of Website	Information Leaked
General (Google, Facebook, Youtube, Yahoo, etc.)	Queries, profile photos, video contents, searches
Political (State Magazine, NewsMax, etc.)	Full content of website, login page
Sports (ESPN, NBA, MLB, Yahoo Sports, etc.)	Full content

Travel (Booking.com, TripAdvisor, Expedia, etc.)	Queries, location, website name
Sexual Orientation (The Advocate, Gay.com, etc.)	Full content
Health (NIH, WebMD, MayoClinic, etc.)	Website content, full content, website name
Shopping (eBay, Netflix, Amazon, Groupon, etc.)	Items viewed, recently viewed, location, sign up
News (NY Times, The Weather Channel, etc.)	Full content, website name
Religion (Bible Gateway, Parallel Bible, etc.)	Full content, query string
Financial (PayPal, American Express, Chase etc.)	Nothing (https)

This information can be leaked based on traffic monitoring by third party advertisers. Cheng et al. discovered that privacy leakage when connected to some airport hotspots can be up to 68%. The mobile device's name is broadcasted each time it searches for Wi-Fi, which many users are not aware of. The device name alone is capable of leading to the leakage of private information. Moreover, in the 625 usernames detected by Cheng et al., 587 were leaked just by the broadcasts of the mobile devices searching for hotspots (p. 2775). Once the device connected to the public Wi-Fi, personal information can then be collected to profile and possibly locate the user.

In sum, your phone sends out a device name when it searched for a connection. "Jerry's iPhone" reveals your name to anyone within communication range. Connecting your device to a public Wi-Fi sends all of your traffic to the hotspot and opens the door for eavesdropping or packet-sniffing. This can reveal information such as hobbies, interests, where you live (if you search news sites), where you shop, what you look like (in the case of sharing photos), and other identifying factors that could help a social engineer piece together who you are. Public Wi-Fi hosts do not always—if ever—take the steps necessary to secure your privacy; protecting your private information is therefore up to you.

Not Just in the Airport, But on the Plane

Recently, there has been controversy over whether Apple should open up their technology to the FBI so the government could more efficiently locate terrorists. Reporters have been eager to cover the details as the story unfolds. It is not uncommon for them, as for other businesspeople or students, to continue working on flights. Thanks to the popularity of Wi-Fi, airlines have been able to offer it to their customers in the air.

This Wi-Fi is public, just as it would be on the ground. While users may not consider the privacy of in-flight Wi-Fi—they are practically alone in the air, so who would hack them?—their information is just as exposed as if they used open public Wi-Fi down on Earth.

One reporter was the victim of this in February 2016 (Petrow). In Steven Petrow's case, his hacker tapped him on the shoulder after the flight to let him know that he was able to see all of the emails that he sent and received. His hacker admitted to doing this to most people on the flight. It is ironic that a reporter who had been writing a story about iPhones being hacked by the government was hacked in the process by a fellow traveler.

The reason the hacker stepped up to the reporter after the incident was because he felt that the story the reporter was planning to write had to be shared: by opening up the technology to the FBI, Apple would have to reduce the security of its devices. Apple would have to create a hole in their security for the agents to get through; but this hole would have to remain open. This would make the danger of getting hacked even more prevalent. This could mean the exposure of more sensitive data, and possibly increase the number of identities stolen if iPhone use persists as it does today.

The provider of the internet access, Gogo, cautioned in the aftermath that sensitive data should not be accessed unless security measures such as a VPN are in place. In an age where so

much of our lives is digitized, it is important to recognize that nothing is fully secure. Everything you do while connected to a public Wi-Fi hotspot can be monitored.

Compromising Communication in the OSI Model

In 2006, Bruce Potter, founder of the non-profit think-tank titled the Shmoo Group of security professionals, published an article in *Communications of the ACM – Hacking and Innovation*. He titled it: "Wireless hotspots: petri dish of wireless security." He asserted that obtaining a fully secure connection with a public hotspot was impossible.

Corporate Wi-Fi, where employees are the only users allowed to tap into the access points, is the exception. These typically use what is called bidirectional certificate-based authentication architecture. In this, both the clients and the infrastructure maintain security. This is pricey and difficult to assemble. It is even more difficult to maintain, as it requires centralized control.

In an Open Systems Interconnection (OSI) network model, there are seven layers: 1. Physical, 2. Data Link, 3. Network, 4. Transport, 5. Session, 6. Presentation, and 7. Application. These seven layers provide a conceptual model of how systems communicate. It starts with the physical layer, which is responsible for transmitting and receiving unstructured raw data in zeroes and ones through physical hardware such as wires and cables. This is what becomes compromised as soon as you connect to public Wi-Fi. What does that mean?

Without going into the specifics, the seven layers talk to each other. After the physical layer, the data link layer assigns protocols to the data and defines its packet sequencing. The network layer applies logical protocols so that the recipient can understand the data, as well as use routers to manage traffic. The transport layer takes care of the data as it travels from one point to another. It makes sure that the data is sent and received error-free. The session layer

maintains the dialogue between systems in that it manages the opening and closing of connections. The presentation layer makes sure that the network can understand the data and encrypts/decrypts it. Finally, the application layer is the interface layer.

Each layer poses its own type security. For example, the network layer is where your firewalls are. In a wired network, a hacker would have to start at the bottom: the physical layer. However, in a Wi-Fi network, the physical location of the system and user are irrelevant. Wi-Fi networks can be accessed from various locations expanding considerable distances. Even if a social engineer did not set up the hotspot you connect to, a hacker might very well be monitoring the hotspot with downloadable software that allows them to intercept data that your system transmits. Furthermore, from an OSI perspective, wireless networks allow hackers to skip level 1, giving them a leg-up on getting your information.

Online Trust and the Optimistic Bias

In 2004, Wang and Emurian of the University of Maryland, Baltimore County overviewed online trust using these dimensions: graphic design, structure design, content design, and social-cue design. They argued that by improving these dimensions, online merchants could better gain the trust of consumers. At this time, 64% of consumers "expressed reservations about trusting e-commerce sites," according to Princeton Survey Research Associates (2002), (Wang, p. 106). Furthermore, the Pew Internet and American Life Project (PIP) revealed that 68% of consumers were hesitant to reveal financial information and only 48% had used a credit card in an online purchase.

Flash-forward to today. Dyn, a cloud-based Internet Performance company, released their "2015 Report: Global Consumer Online Shopping Expectations," which indicates that online trust has shifted. They report: "More than 90% of consumers surveyed said they make at least

25% of their purchases online," (Dyn, 2015, p. 2). The 48% of users that had used a credit card to make an online purchase in 2002 has now more than doubled to 90% in 2015.

Dyn also revealed that 86% of participants' trust is affected by the speed and performance of the website (p. 2). This is an interesting statistic that could be translated to the context of why users choose to connect to public Wi-Fi. Recall that one of the factors I named as contributive to why people trust Wi-Fi is its ease of use. The more user-friendly something is, the more people feel inclined to trust it. That is it say, if someone connects to Wi-Fi that is running slowly, they are more likely to become hesitant and disconnect. If someone connects to Wi-Fi that is speedy, they are more likely to remain connected and trust that connection.

Those theories and statistics work for e-commerce, but can they be transferred to make sense for why people trust hotspots? Not exactly, but they can certainly be used to develop theories that work for hotspot trustworthiness.

The concept of trust is essentially the same in all contexts, although the degree to which someone is required to exhibit trust varies. In e-commerce transactions, shoppers may be more likely to stop and consider their actions. They know the consequences of a bad transaction: they risk their credit card number being stolen or they risk paying for an item that will never come. As I mentioned at the beginning of this paper, there are four factors of trust; one of those factors is knowledge of associated risks. This is one thing that may be lacking from users of public Wi-Fi.

However, Private Communications Corporations may disagree. Their publication, "Whitepaper: The Hidden Dangers of Public WiFi" (2014) indicates that 88% of surveyed adults think that identity theft could be a potential issue with using public Wi-Fi (p. 6). They also mentioned that 76% of those surveyed acknowledged the possibility of a compromised account and 39% mentioned fraudulent tax filing (p. 6). So if users *do* know the risks, and are afraid of

them, why do they still access bank accounts, emails, bills, taxes, etc. from a public Wi-Fi connection?

It is extremely common for people to take on a "It Will Never Happen to Me" mentality, otherwise known as the optimistic bias. Most people have probably read at least one or two stories that warn against using public Wi-Fi. Why do they continue to use it without careful consideration? The optimistic bias. For some—if not most—being the victim of a hack or social engineering attack while connected to public Wi-Fi could be as likely as their being attacked by a bear while on a leisurely stroll: "It will never happen to me."

Furthermore, behavioral scientists Neil Weinstein and William Klein (2015) reported, "Across a variety of hazards, it is common to find 40–70% of a group asserting below average risk; another 30–50% saying that their risk is average; and less than 10% acknowledging that their risk is above average," (p. 699). Unfortunately for those 70% that believe they are at a "below average" risk, hacks and social engineering attacks happen every day; so unless the hackers are targeting the same 30% of the population over and over again, they are likely to experience an attack on themselves at some point. Of course, this data does not translate perfectly into the realm of social engineering and online privacy, but it provides accurate insight into the affect the optimistic bias has on users. Evidently, risk perception is skewed.

If there has been a lack in effort creating awareness of the dangers of public Wi-Fi, there has certainly been a lack in effort fighting the associated optimistic bias. Users need to know that it *can* happen to them. Private Communications point to an increasingly obvious solution: use of a VPN. They suggest that this is "the only way" for users to be protected on public connections (2014, p. 9). Individuals as well as businesses tend to "ensure" their security using firewalls and

security software; but this actually does not actually ensure the security of their information at all on public Wi-Fi connections.

A VPN acts as an encryption tunnel, through which your information can travel safely without penetration. Users who say “It can never happen to me,” are much more likely to be correct if they make use of a VPN.

Implications of the Optimistic Bias with Online Privacy

Cho, Lee, and Chung (2010) set out to explain the cognitive aspect involved in the risk judgments of users using a sample of 910 people in the Singapore area. They found that individuals perceive risk at the personal and societal levels and that when it comes to online privacy risks, users tend to be susceptible to a strong optimistic bias. They also found that this optimistic bias is moderated by the user’s “perceived controllability” and “prior experience.” Perceived controllability refers to the level of control users feel that they have over their online privacy. Prior experience refers to the exposure users have had to threats and their prevention methods, as well as their familiarity with online activities. Cho, Lee, and Chung primarily hypothesized that users felt they were less vulnerable to online privacy risks than their peers.

Their telephone survey results supported their hypothesis (2010). They found that the existing literature on the role of the optimistic bias in social risk held true for the newer online privacy social risk. After splitting the group in two (456 and 454 participants), they assigned the former group to a low level of perceived controllability and the latter group to a high level of it. From there, the groups were divided into levels of prior experience with general privacy issues and SPAM—none, low, or high. Performing this for both personal and societal levels of risk, Cho, Lee, and Chung were able to conclude that online privacy risks are absolutely impacted by the optimistic bias.

Methodology

If online privacy in its most general sense is impacted by optimistic bias, then I hypothesize that the decision to connect to a public Wi-Fi hotspot must also be affected by the optimistic bias. Therefore, vulnerability to social engineering is in part due to the user's susceptibility to a strong enough optimistic bias.

Where does the optimistic bias fit in with trust? Is it trust? The phenomenon of the optimistic bias is a cognitive heuristic—it is not an implication of trust. It is, however, worth considering in the context of this paper. While the four factors of trust may not explain why the entirety of users connect and expose themselves on public Wi-Fi, adding optimism to the equation might.

Trust + Optimistic Bias = Vulnerability to Social Engineering

This is the equation that I propose as my hypothesis. If trust is not enough to sway people to expose themselves on public Wi-Fi, but the optimistic bias alone is not enough to account for the masses; then a combination of the two is the answer.

To better understand the role that trust and the optimistic bias plays in why people connect to public Wi-Fi, I used an online survey via Qualtrics. The survey was offered to two sections of MIS304, comprised of third year Eller College students at the University of Arizona. At the time of analysis, 167 students had completed the survey (n = 167). Participation in the survey was completely voluntary and without penalty. The names of the students were deleted from the data and will further not be associated with the data they have contributed.

To measure trust in the participants, I chose to use two factors of trust that I have mentioned: physical location of the user and credibility of the network name. These factors were used as variables in scenarios that were randomly assigned to participants. The network name

was varied in familiarity to the user. For example, users given the scenario of attending a University of Arizona basketball game at McKale Center were prompted with "McKale Wi-Fi," which would be a familiar name to the user. I also chose to look at the impact of duration of time spent on network (just for a second or for the duration of the time spent at the location specified in the scenarios). This factor could be used to evaluate whether users connect to public Wi-Fi or not.

Each scenario was designed with a high or low level of the three factors: location, name, and duration. High, in the sense of location and name, means a strong sense of familiarity to the user. Low means zero to no familiarity. A high level of duration corresponds to a short amount of time spent on the network; a low level of duration corresponds to a longer amount of time. This is because users may feel more compelled (higher likelihood) to connect if they sense that they are exposing themselves less in the shorter amount of time. For the purposes of statistical evaluation, high was assigned a value of 1 and low a value of 0.

To measure the degree of optimism in users, participants were presented with a series of questions that asked them to assign a likelihood of risk to themselves and a likelihood of risk to others. "Others" was defined for the participants as "other people who are about your age and have similar social positions or jobs," (Cho et al., 2010, p. 990). Responses were based on a 7-point Likert scale, with 1 = extremely likely and 7 = extremely unlikely.

The survey scenarios and sample measures that have been directly referenced in this paper can be found in Appendix I and II at the end of this document.

Results

Considering the factor of familiar Wi-Fi (credibility appearance factor of trust), regardless of the duration and physical location, the null is the number of users that connect to

public Wi-Fi in the basketball setting = the number of users that connect to public Wi-Fi in the concert setting (no significance). For this test, a value of 1 is assigned to a decision to connect, and 0 is assigned to a decision not to connect. With means of 0.795 and 0.446 respectively, a paired t-test revealed $t = 5.561$, $p < 0.001$. The null is therefore rejected; the number of users that connect in each setting is not equal.

In a similar test, with 1 = connection and 0 = no connection, basketball games were compared to coffee cafes. The null is the number of users that connect to public Wi-Fi in the basketball setting = the number of users that connect to public Wi-Fi in the café setting (no significance). The mean of basketball game was 0.795 and the mean of the café was 0.639. With $t = 2.6964$, $p < 0.01$ in a paired t-test, the null is rejected again. Keep in mind that this is regardless of duration and location.

Next consider the contrast between a known café (i.e. Starbucks) and an unknown café (i.e. Serenity). In a two sample t-test, familiar Wi-Fi significance was tested in both of the familiar and unfamiliar locations. The null is the same number of users that connect to Wi-Fi in Starbucks will connect in Serenity if the Wi-fi name is familiar (no significance). Where 1 = connection and 0 = no connection, the mean of Starbucks ("Google Starbucks Wi-Fi") was 0.5 and the mean of Serenity Café ("Serenity WiFi") was 0.7804878. From this, $t = 2.7467$, $p < 0.01$. Therefore, I reject the null. Conversely, unfamiliar Wi-Fi names in both locations. The null for this test is the same number of users will connect in Starbucks as in Serenity even though the Wi-Fi name is unfamiliar. I reject this null. To obtain this result, the means of Starbucks ("COFFEE WIFI") and Serenity Café (also "COFFEE WIFI") were 0.1666667 and 0.6190476, respectively resulting in $t = 4.7320$, $p < 0.001$.

The optimistic bias—i.e. comparison of "you" (self) and "others"—t-test revealed results of $t = 12.0112$, $p < 0.001$. The null is the probability of consequences for yourself is the same as the probability of consequences for others. Due to the values from the t-test, I reject this null. The mean of "you," in which a lower average equates to a higher likeliness of risk, is 3.592814; the mean of "others" is 2.491018. Again, this is based on a 7-point Likert scale in which 1 = extremely likely and 7 = extremely unlikely.

Considering the basketball game setting in my proposed scenarios, a multiple regression analysis was done to test the significance of the variables. This was done with an ANOVA. The original ANOVA used a global F test to see if the null hypothesis of Beta=0 could be rejected and to identify significance. With the multiple regression analysis, I rejected the null and concluded that some of the variables did prove significant in the test. Individual t-tests were used to decipher which variables held significance (Figure 1). Those tests revealed that the variables of familiarity (FAMIWIFI), optimism, and gender held significance. With that in mind, if I were to rerun this experiment again, I would test using only those variables as those are the ones that hold significance.

In order for a factor to be significant at a 95% confidence interval, the p-value must be less than 0.05. Looking first at the Wi-Fi name familiarity (credibility appearance factor of trust), $t = 3.24$ with a p-value of 0.001. The location (physical location of the user factor of trust) revealed $t = -0.22$ with a p-value of 0.826. Duration revealed $t = 0.04$ with a p-value of 0.971. Optimism held $t = -4.06$ with a p-value of 0.000. Age held $t = 0.64$ with a p-value of 0.526. Finally, gender had values of $t = 2.13$ with $p = 0.034$. These values can be referenced in the below table under the columns labelled "t" and "P>| t |".

BBALL1	Coef.	Std. Err.	t	P>|t|	[95% Conf.	Interval]
FAMWIFI	.2201621	.0679644	3.24	0.001	.0859391	.3543851
LOC	-.0149092	.0677977	-0.22	0.826	-.148803	.1189845
DUR	.0024216	.0676398	0.04	0.971	-.1311603	.1360035
optimism	-.1164356	.0286782	-4.06	0.000	-.1730723	-.059799
Age	.0182535	.0287023	0.64	0.526	-.0384308	.0749378
Gender	.142348	.0667172	2.13	0.034	.0105881	.2741079
_cons	.1062644	.6295184	0.17	0.866	-1.136973	1.349501

Figure 1

To more specifically look at the optimistic bias, I have compiled a bar graph with the responses from the participants (Figure 2). In each question, participants consistently placed themselves in a higher regard. The higher the number, the less likely the susceptibility to the risk of social engineering. As previously mentioned, these results are a product of a 7-point Likert scale in which 1 = extremely likely and 7 = extremely unlikely. The mean of responses for questions relating “you” to consequences was 3.592814 (between “slightly unlikely” and “neither likely nor unlikely”); and the mean for questions relating “others” to consequences was 2.491018 (between “moderately likely” and “slightly likely”).

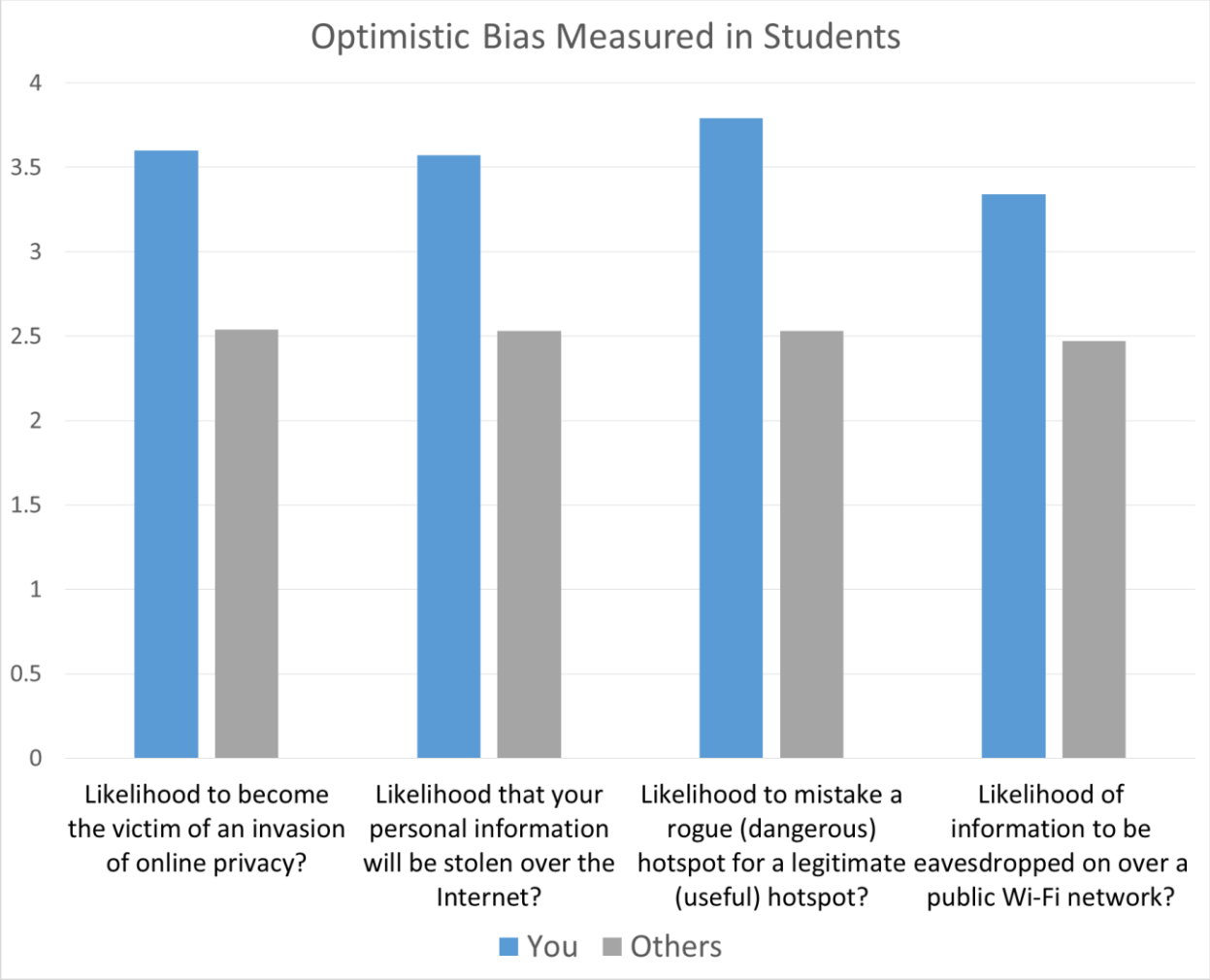

Figure 2

Analysis and Conclusion

For each of the aforementioned tests, I have rejected the null hypothesis. In the following analysis, it is important to remember that correlation does not imply causation. However, these results have p-values < 0.05, and are therefore supportive of my original hypothesis: factors of trust and the optimistic bias work together in a user's decision to connect to public Wi-Fi, leaving them vulnerable to social engineering.

In the first results, familiar Wi-Fi, regardless of duration and location, proved to be a significant variable. The Wi-Fi names in the scenarios were McKale Wi-Fi, ASU Wi-Fi, and Verizon Wi-Fi. All three of these names are recognizable to the user, and therefore could be

perceived as credible. However, although the Verizon Wi-Fi is based on a familiar name, it is not based on the arena's name—Talking Stick. Therefore, it is possible that the users could have perceived it as a fake connection, thus impacting the results and suggesting that a familiar and credible network name is a significant variable that users could consider when making the decision to connect to public Wi-Fi.

Reference List

2015 Global Consumer Online Shopping Expectations - Dyn. (2015, February 12). Retrieved March 2, 2016, from http://pages.dyn.com/rs/dyn/images/Dyn 2015 Report-Global Consumer Online Shopping Expectations.pdf?aliId=13210311

Whitepaper: October 2014 - The Hidden Dangers of Public WiFi – Private Communications Corporation. (2014, October). Retrieved March 14, 2016, from http://www.privatewifi.com/wp-content/uploads/2015/01/PWF_whitepaper_v6.pdf

Cheng, N., Wang, X. O., Cheng, W., Mohapatra, P., & Seneviratne, A. (2013). Characterizing privacy leakage of public WiFi networks for users on travel. *2013 Proceedings IEEE INFOCOM*, 2769-2777. Retrieved January 27, 2016.

Cho, H., Lee, J., & Chung, S. (2010). Optimistic bias about online privacy risks: Testing the moderating effects of perceived controllability and prior experience. *Computers in Human Behavior, 26*(5), 987-995. doi:10.1016/j.chb.2010.02.012

Compeau, D. R., & Higgins, C. A. (1995). Application of Social Cognitive Theory to Training for Computer Skills. *Information Systems Research, 6*(2), 118-143. doi:10.1287/isre.6.2.118

Corritore, C. L., Kracher, B., & Wiedenbeck, S. (2003). On-line trust: Concepts, evolving themes, a model. *International Journal of Human-Computer Studies, 58*(6), 737-758. Retrieved January 28, 2016.

Higgs, L. (2013, July 01). Free Wi-Fi? Beware of security risks. Retrieved February 15, 2016, from http://www.usatoday.com/story/tech/2013/07/01/free-wi-fi-risks/2480167/

Kline, A., & Strickler, J. (1993). Perceptions of risk for AIDS among women in drug treatment. *Health Psychology, 12*(4), 313-323. doi:10.1037/0278-6133.12.4.313

Mitnick, K. D., & Simon, W. L. (2002). *The art of deception: Controlling the human element of security*. Indianapolis, IN: Wiley Pub.

Petrow, S. (2016, February 24). "I got hacked mid-air while writing an Apple-FBI story." Retrieved February 25, 2016, from http://www.usatoday.com/story/tech/columnist/2016/02/24/got-hacked-my-mac-while-writing-story/80844720/

Potter, B. (2006). Wireless Hotspots: Petri Dish of Wireless Security. *Communications of the ACM Commun. ACM*, *49*(6), 50. Retrieved February 16, 2016.

Tyler, T. R., & Cook, F. L. (1984). The mass media and judgments of risk: Distinguishing impact on personal and societal level judgments. *Journal of Personality and Social Psychology, 47*(4), 693-708. doi:10.1037/0022-3514.47.4.693

Wang, Y. D., & Emurian, H. H. (2005). An overview of online trust: Concepts, elements, and implications. *Computers in Human Behavior*, *21*(1), 105-125. Retrieved March 1, 2016.

Wei, R., Lo, V., & Lu, H. (2007). Reconsidering the Relationship Between the Third-Person Perception and Optimistic Bias. *Communication Research, 34*(6), 665-684. doi:10.1177/0093650207307903

Weinstein, N. D., & Klein, W. M. (1995). Resistance of personal risk perceptions to debiasing interventions. *Health Psychology, 14*(2), 132-140. doi:10.1037/0278-6133.14.2.132

Weinstein, N. D., & Klein, W. M. (2015). Health Risk Appraisal and Optimistic Bias. *International Encyclopedia of the Social & Behavioral Sciences*, 698-701. Retrieved March 28, 2016.

APPENDIX I: Survey Scenarios

Students received one of the following scenarios:

Familiar location, familiar name, long duration

1.) You are at the UA vs. ASU basketball game at McKale Center. Because you are a student, you entered the ZonaZoo section almost two hours before the game. The game is sold out because of the rivalry between the two teams. To keep busy before the game, you scroll through various social media. You notice that as McKale fills up and more people go on their phones, your UAWiFi signal gets weaker. Come the start of the game, you cannot even open up your ZonaZoo app to check-in and get points for attending. Using LTE doesn't work because the app needs a more specific approximation of your location to make sure you're at the game. You pull up your Wi-Fi connections and see "McKale Wi-Fi." You consider connecting for the duration of the game.

2.) You go to see a concert at Talking Stick Resort Arena in downtown Phoenix which is your favorite venue for concerts. Because of the number of people connected to the internet, your network is running slowly. You have tried reposting your Instagram picture three times now, and all you want to do is get it posted so your friends can see how great the concert is. You check your connections and see several locked networks and one open network: "Verizon WiFi." You consider connecting for the duration of the concert.

3.) You enter a Starbucks in Tucson and order a latte. You frequent Starbucks, so the store is familiar. You and your friends spot a table in the corner and you all settle in to catch up for the next hour or so. The latte is one of the best you've had. You pull up your Wi-Fi connections and see "Google Starbucks" WiFi. You consider connecting for the duration of your Starbucks visit.

4.) You have a layover at the Houston airport, which you have been to once before. The Houston Airport System (HAS) is big, but not big enough to keep you busy for two hours until your next flight. After getting food and checking out the gift shops, you take a seat at your gate and pull out your phone. Because you are traveling, you don't want to use up too much data too quickly. You open up your connections and see "HAS WIFI." You consider connecting for the duration of your layover.

Familiar location, familiar name, short duration

1.) You are at the UA vs. ASU basketball game at McKale Center. Because you are a student, you entered the ZonaZoo section almost two hours before the game. The game is sold out because of the rivalry between the two teams. To keep busy before the game, you scroll through various social media. You notice that as McKale fills up and more people go on their phones, your UAWiFi signal gets weaker. Come the start of the game, you cannot even open up your ZonaZoo app to check-in and get points for attending. Using LTE doesn't work because the app needs a more specific approximation of your location to make sure you're at the game. You pull up your Wi-Fi connections and see "McKale Wi-Fi." You consider connecting for just a second—just long enough to check-in.

2.) You go to see a concert at Talking Stick Resort Arena in downtown Phoenix which is your favorite venue for concerts. Because of the number of people connected to the internet, your network is running slowly. You have tried reposting your Instagram picture three times now, and all you want to do is get it posted so your friends can see how great the concert is. You check your connections and see several locked networks and one open

network: “Verizon WiFi.” You consider connecting for just a second—just long enough to post to Instagram.

3.) You enter a Starbucks in Tucson and order a latte. You frequent Starbucks, so the store is familiar. You and your friends spot a table in the corner and you all settle in to catch up for the next hour or so. The latte is one of the best you’ve had. You pull up your Wi-Fi connections and see “Google Starbucks” WiFi. You consider connecting for just a second—just long enough to post a snapchat.

4.) You have a layover at the Houston airport, which you have been to once before. The Houston Airport System (HAS) is big, but not big enough to keep you busy for two hours until your next flight. After getting food and checking out the gift shops, you take a seat at your gate and pull out your phone. Because you are traveling, you don’t want to use up too much data too quickly. You open up your connections and see “HAS WIFI.” You consider connecting for just a second—just long enough to check your email.

Familiar location, unfamiliar name, long duration

1.) You are at the UA vs. ASU basketball game at McKale Center. Because you are a student, you entered the ZonaZoo section almost two hours before the game. The game is sold out because of the rivalry between the two teams. To keep busy before the game, you scroll through various social media. You notice that as McKale fills up and more people go on their phones, your UAWiFi signal gets weaker. Come the start of the game, you cannot even open up your ZonaZoo app to check-in and get points for attending. Using LTE doesn’t work because the app needs a more specific approximation of your location to make sure you’re at the game. You pull up your Wi-Fi connections and see “GAME WIFI.” You consider connecting for the duration of the game.

2.) You go to see a concert at Talking Stick Resort Arena in downtown Phoenix which is your favorite venue for concerts. Because of the number of people connected to the internet, your network is running slowly. You have tried reposting your Instagram picture three times now, and all you want to do is get it posted so your friends can see how great the concert is. You check your connections and see several locked networks and one open network: "Concert WiFi." You consider connecting for the duration of the concert.

3.) You enter a Starbucks in Tucson and order a latte. You frequent Starbucks, so the store is familiar. You and your friends spot a table in the corner and you all settle in to catch up for the next hour or so. The latte is one of the best you've had. You pull up your Wi-Fi connections and see "COFFEE WIFI." You consider connecting for the duration of your Starbucks visit.

4.) You have a layover at the Houston airport, which you have been to once before. The Houston Airport System (HAS) is big, but not big enough to keep you busy for two hours until your next flight. After getting food and checking out the gift shops, you take a seat at your gate and pull out your phone. Because you are traveling, you don't want to use up too much data too quickly. You open up your connections and see "Free Airport WIFI." You consider connecting for the duration of your layover.

Familiar location, unfamiliar name, short duration

1.) You are at the UA vs. ASU basketball game at McKale Center. Because you are a student, you entered the ZonaZoo section almost two hours before the game. The game is sold out because of the rivalry between the two teams. To keep busy before the game, you scroll through various social media. You notice that as McKale fills up and more

people go on their phones, your UAWiFi signal gets weaker. Come the start of the game, you cannot even open up your ZonaZoo app to check-in and get points for attending. Using LTE doesn't work because the app needs a more specific approximation of your location to make sure you're at the game. You pull up your Wi-Fi connections and see "GAME WIFI." You consider connecting for just a second—just long enough to check-in.

2.) You go to see a concert at Talking Stick Resort Arena in downtown Phoenix which is your favorite venue for concerts. Because of the number of people connected to the internet, your network is running slowly. You have tried reposting your Instagram picture three times now, and all you want to do is get it posted so your friends can see how great the concert is. You check your connections and see several locked networks and one open network: "Concert WiFi." You consider connecting for just a second—just long enough to post to Instagram.

3.) You enter a Starbucks in Tucson and order a latte. You frequent Starbucks, so the store is familiar. You and your friends spot a table in the corner and you all settle in to catch up for the next hour or so. The latte is one of the best you've had. You pull up your Wi-Fi connections and see "COFFEE WIFI." You consider connecting for just a second—just long enough to post a snapchat.

4.) You have a layover at the Houston airport, which you have been to once before. The Houston Airport System (HAS) is big, but not big enough to keep you busy for two hours until your next flight. After getting food and checking out the gift shops, you take a seat at your gate and pull out your phone. Because you are traveling, you don't want to use up too much data too quickly. You open up your connections and see "Free

Airport WIFI." You consider connecting for just a second—just long enough to check your email.

Unfamiliar location, familiar name, long duration

1.) You are at the UA vs. ASU basketball game at Arizona State. Because you are a student, you entered the visitors section almost two hours before the game. The game is sold out because of the rivalry between the two teams. To keep busy before the game, you scroll through various social media. You notice that as stadium fills up and more people go on their phones, your LTE signal gets weaker. You pull up your Wi-Fi connections and see "ASU Wi-Fi." You consider connecting for the duration of the game.

2.) You go to see a concert at Talking Stick Resort Arena in downtown Phoenix, your first time at the resort. Because of the number of people connected to the internet, your network is running slowly. You have tried reposting your Instagram picture three times now, and all you want to do is get it posted so your friends can see how great the concert is. You check your connections and see several locked networks and one open network: "Verizon WiFi." You consider connecting for the duration of the concert.

3.) You enter a new coffee shop called Café Serenity in downtown Tucson and order a latte. Your friends noticed this café as you were walking around. It is not a chain coffee house like Starbucks or The Coffee Bean, it's more of a mom and pop place. The latte is one of the best you've had. You pull up your Wi-Fi connections and see "Serenity WiFi." You consider connecting for the duration of your visit to the café.

4.) You have a layover at the Houston airport, which you have never visited before. The Houston Airport System (HAS) is big, but not big enough to keep you busy for two

hours until your next flight. After getting food and checking out the gift shops, you take a seat at your gate and pull out your phone. Because you are traveling, you don't want to use up too much data too quickly. You open up your connections and see "HAS WIFI." You consider connecting for the duration of your layover.

Unfamiliar location, familiar name, short duration

1.) You are at the UA vs. ASU basketball game at Arizona State. Because you are a student, you entered the visitors section almost two hours before the game. The game is sold out because of the rivalry between the two teams. To keep busy before the game, you scroll through various social media. You notice that as stadium fills up and more people go on their phones, your LTE signal gets weaker. You pull up your Wi-Fi connections and see "ASU Wi-Fi." You consider connecting for just a second—just long enough to check social media updates.

2.) You go to see a concert at Talking Stick Resort Arena in downtown Phoenix, your first time at the resort. Because of the number of people connected to the internet, your network is running slowly. You have tried reposting your Instagram picture three times now, and all you want to do is get it posted so your friends can see how great the concert is. You check your connections and see several locked networks and one open network: "Verizon WiFi." You consider connecting for just a second—just long enough to upload your picture.

3.) You enter a new coffee shop called Café Serenity in downtown Tucson and order a latte. Your friends noticed this café as you were walking around. It is not a chain coffee house like Starbucks or The Coffee Bean, it's more of a mom and pop place. The latte is one of the best you've had. You pull up your Wi-Fi connections and see

"Serenity WiFi." You consider connecting for just a second—just long enough to post to snapchat.

4.) You have a layover at the Houston airport, which you have never visited before. The Houston Airport System (HAS) is big, but not big enough to keep you busy for two hours until your next flight. After getting food and checking out the gift shops, you take a seat at your gate and pull out your phone. Because you are traveling, you don't want to use up too much data too quickly. You open up your connections and see "HAS WIFI." You consider connecting for just a second—just long enough to check your email.

Unfamiliar name, unfamiliar location, long duration

1.) You are at the UA vs. ASU basketball game at Arizona State. Because you are a student, you entered the visitors section almost two hours before the game. The game is sold out because of the rivalry between the two teams. To keep busy before the game, you scroll through various social media. You notice that as stadium fills up and more people go on their phones, your LTE signal gets weaker. You pull up your Wi-Fi connections and see "GAME Wi-Fi." You consider connecting for the duration of the game.

2.) You go to see a concert at Talking Stick Resort Arena in downtown Phoenix, your first time at the resort. Because of the number of people connected to the internet, your network is running slowly. You have tried reposting your Instagram picture three times now, and all you want to do is get it posted so your friends can see how great the concert is. You check your connections and see several locked networks and

one open network: “Concert WiFi.” You consider connecting for the duration of the concert.

3.) You enter a new coffee shop called Café Serenity in downtown Tucson and order a latte. Your friends noticed this café as you were walking around. It is not a chain coffee house like Starbucks or The Coffee Bean, it’s more of a mom and pop place. The latte is one of the best you’ve had. You pull up your Wi-Fi connections and see “COFFEE WIFI.” You consider connecting for the duration of your visit to the café.

4.) You have a layover at the Houston airport, which you have never visited before. The Houston Airport System (HAS) is big, but not big enough to keep you busy for two hours until your next flight. After getting food and checking out the gift shops, you take a seat at your gate and pull out your phone. Because you are traveling, you don’t want to use up too much data too quickly. You open up your connections and see “Free Airport WIFI.” You consider connecting for the duration of your layover.

Unfamiliar location, unfamiliar name, short duration

1.) You are at the UA vs. ASU basketball game at Arizona State. Because you are a student, you entered the visitors section almost two hours before the game. The game is sold out because of the rivalry between the two teams. To keep busy before the game, you scroll through various social media. You notice that as stadium fills up and more people go on their phones, your LTE signal gets weaker. You pull up your Wi-Fi connections and see “GAME Wi-Fi.” You consider connecting for just a second—just long enough to check social media updates.

2.) You go to see a concert at Talking Stick Resort Arena in downtown Phoenix, your first time at the resort. Because of the number of people connected to the internet,

your network is running slowly. You have tried reposting your Instagram picture three times now, and all you want to do is get it posted so your friends can see how great the concert is. You check your connections and see several locked networks and one open network: “Concert WiFi.” You consider connecting for just a second—just long enough to post to Instagram.

3.) You enter a new coffee shop called Café Serenity in downtown Tucson and order a latte. Your friends noticed this café as you were walking around. It is not a chain coffee house like Starbucks or The Coffee Bean, it’s more of a mom and pop place. The latte is one of the best you’ve had. You pull up your Wi-Fi connections and see “COFFEE WIFI.” You consider connecting for just a second—just long enough to post to snapchat.

4.) You have a layover at the Houston airport, which you have never visited before. The Houston Airport System (HAS) is big, but not big enough to keep you busy for two hours until your next flight. After getting food and checking out the gift shops, you take a seat at your gate and pull out your phone. Because you are traveling, you don’t want to use up too much data too quickly. You open up your connections and see “Free Airport WIFI.” You consider connecting for just a second—just long enough to check your email.

APPENDIX II: Survey Measures

Intention to connect to public Wi-Fi (strongly disagree to strongly agree)

I intend to connect to public Wi-Fi in the near future.

If I have a chance, I will connect to public Wi-Fi.

I never connect to public Wi-Fi.

Subjective norm

If I connect to a public Wi-Fi hotspot, most of the people who are important to me would disapprove.

Most people who are important to me would look down on me if I connected to a public Wi-Fi hotspot.

No one who is important to me thinks it is okay to connect to a public Wi-Fi hotspot.

My colleagues think connecting to a public Wi-Fi hotspot is wrong.

Attitude toward public Wi-Fi hotspots (strongly disagree to strongly agree)

To me, connection to public Wi-Fi is a (extremely good—extremely bad) idea.

To me, connection to public Wi-Fi is a (extremely pleasant—extremely unpleasant) idea.

To me, connection to public Wi-Fi is a (extremely wise—extremely unwise) idea.

To me, connection to public Wi-Fi is a (extremely attractive—extremely unattractive) idea.

Perceived behavioral control (strongly disagree to strongly agree)

For me, it is easy to connect to public Wi-Fi.

I have the knowledge and ability to make use of public Wi-Fi hotspots.

I could find public Wi-Fi connections if I wanted to.

Connecting to public Wi-Fi is entirely within my control.

Perceived vulnerability

(Tyler & Cook, 1984; Wei et al., 2007; Weinstein & Klein, 1995).

Personal-level (*self*) vulnerability estimates were measured using two items:

"How likely are you to become the victim of an invasion of online privacy?"

"How likely is it that your personal information will be stolen over the Internet?"

Additions:

How likely are you to mistake a rogue hotspot for a legitimate hotspot?

How likely is your information to be eavesdropped on over a public Wi-Fi network?

Others was explained to the respondents as meaning "other people who are about your age and have similar social positions or jobs," (Cho et al., 2010, p. 990).

"How likely are others to become the victim of an invasion of online privacy?"

"How likely is it that others personal information will be stolen over the Internet?"

Additions:

How likely are others to mistake a rogue hotspot for a legitimate hotspot?

How likely is the information of others to be eavesdropped on over a public Wi-Fi network?

Perceived controllability

(Compeau & Higgins, 1995; Kline & Strickler, 1993)

"I can protect my privacy online by using privacy enhancing technologies (e.g., encryption, anonymizing software, cookie-blocking technologies, etc.)"

"It is possible to stop online marketers or e-commerce vendors from collecting my personal information."

Additions:

I am comfortable using public Wi-Fi because the websites/apps/etc. that I access come with their own layers of security.

If I do not spend a significant amount of time on public Wi-Fi networks, no one will have time to try to steal my information.

If I do not spend a significant amount of time on public Wi-Fi networks, no one will be able to see my information.

I can protect my privacy online by only connecting to public Wi-Fi in places such as hotels, popular restaurants, concert venues, airports, or other high-traffic locations.