Public WiFi Usage Survey

The Identity Theft Resource Center (ITRC) recently conducted its *Public WiFi Usage Survey* to measure the level of consumer knowledge and usage of public WiFi. The ITRC conducted this survey in order to better understand how consumers perceive and use public WiFi. This information would then be used to heighten consumer awareness about safe usage of public WiFi. There were 377 initial responses.

"While technology seems to be making all of our lives easier, it can also leave us open to unsafe practices in exchange. Many people do not realize that using Internet at your local café can lead to identity theft," said Nikki Junker, Social Media Manager for the ITRC. "The survey results will help the ITRC in developing informative materials and documents for consumers, to help keep them safe while using public WiFi." It is the ITRC's hope that the findings of this survey will provide insight on best practices of public WiFi usage.

Executive Summary:

The following are the results from a survey recently conducted by the ITRC on the level of knowledge and usage surrounding public WiFi. The purpose of this survey was to determine existing public perception related to use of public WiFi sites. The survey was also designed to help the ITRC and partner organizations understand and publicize the risks which face consumers using public WiFi and determine how that risk can be minimized. JiWire reported that within the past year "total WiFi usage has more than doubled, increasing by more than 240% since Q2, 2011."[1] This report notes that this increase is being led by mobile devices, and laptops now account for just 48% of the connected devices.

A recent Kaspersky study indicated that "using public networks became the most common way used to access the Internet…" The Kaspersky study also found "that about 70% of tablet owners and 53% of mobile phone users use free public WiFi hotspots to go online." A table within that report indicated that 55% of all mobile devices were used to access free public WiFi hotspots.[2] This comes as no surprise as the ITRC survey Question 1 indicated that 53% of those surveyed indicated that they used public WiFi at least once a week.

The ITRC study showed that while knowledge of the risk of public WiFi usage is present, much more can and should be done to educate the general public. A large percentage of those surveyed (79%) answered that they believe that use of free public WiFi could lead to identity theft, but only 27% indicated use of a Virtual Private Network (VPN).

"This clearly indicates that in general the public does not recognize the effectiveness and necessity of using a VPN to secure public WiFi connections," said Rex Davis, Director of Operations of the ITRC. "The ITRC has long used VPN connections for access to our company resources, and understands the specific need for using VPN when connecting via public WiFi."

Based on the survey results, greater educational and awareness efforts are needed. As the responses to questions 3 and 7 reflect, over half the respondents appeared to be aware of various methods available

---

[1] *JiWire Mobile Audience Insights Report, Q2 2012. JiWire, Inc. (2012)*
[2] *Digital Consumer's Online Trends and Risks.* Kaspersky Lab ZAO. (2012)

to better secure their information. In Question 3, 58% of respondents reported being aware of the use of VPN's. Unfortunately, Question 3 also indicates that 42% to 65% of the respondents did not recognize these various methods of data protection. Similarly, in Question 7, 56% indicated their awareness of ways to protect sensitive data while using public WiFi sites, but 44% indicated they did not know about or did not believe there were ways to protect their information. We can draw a rough conclusion that approximately 40% of the users of public WiFi are simply not knowledgeable about data protection.
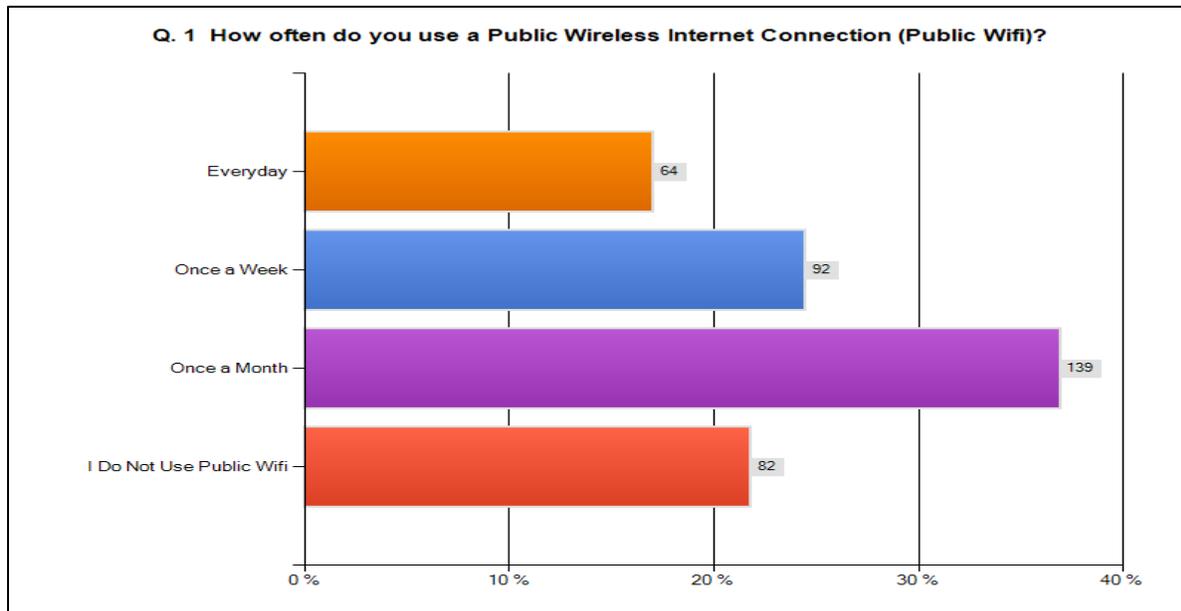
The responses to Questions 4 and 5 of the ITRC survey suggest some additional areas for inquiry. Approximately 8 of 10 respondents in Question 4 indicate that use of a public WiFi could result in identity theft. However, in Question 5, we see that 4 of 10 feel unconcerned, or fairly safe, while 6 of 10 are concerned or very concerned. The contrast between 80% of respondents who believe using public WiFi could result in identity theft versus the 60% who felt concerned when using public WiFi indicates a possible belief that while identity theft may be a risk, it is such a minimal risk that it does not warrant concern. Another question could be, that of the 4 in 10 that feel unconcerned, or fairly safe, do they represent knowledgeable users who have taken security measures, or do they represent those who just have no understanding or knowledge of the risk?

Likely due to the fierce competition to attract customers, many coffee shops and restaurants now offer free public WiFi. Therefore, it is no surprise that 3 out of 4 respondents indicated that they used these free services. Hotels were the second most used location for public WiFi access (54%), followed by airports (38%). In the location category "Other" we noted that a significant number of respondents identified "doctor's offices and hospitals" and "malls and retail outlets." This begs the question whether these WiFi connections are intended to be public, or are simply unprotected connections.
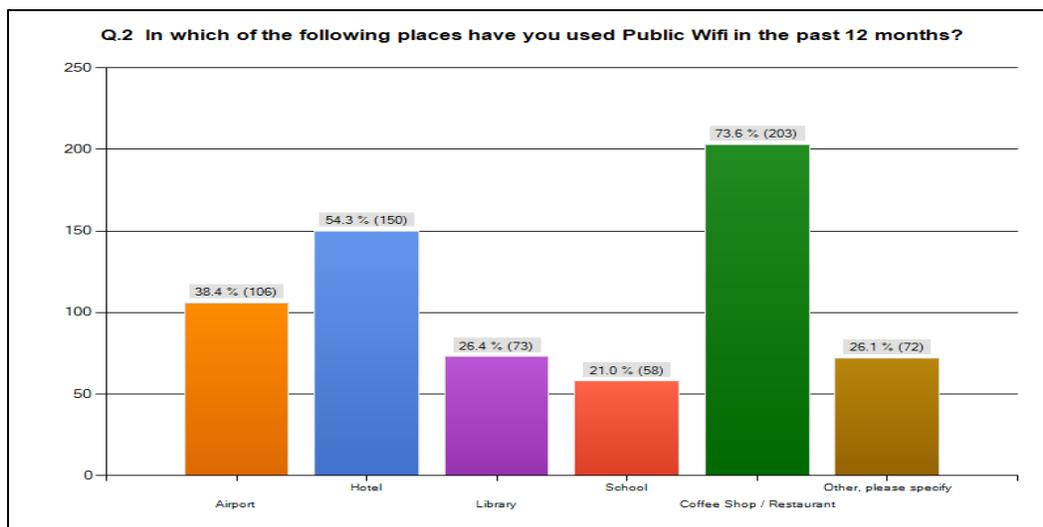
Whether or not these location percentages will change is uncertain, but the fact remains that public WiFi will become more accessible to the average person. For more than a year, state and local governments have been installing public WiFi hotspots at an ever increasing pace. Greater availability of locations will undoubtedly contribute to increased usage. This expected increase in public WiFi activity and access will also no doubt make public WiFi nodes a more important target for data thieves. This problem can only be solved by public awareness and education to create widespread use of readily available privacy solutions.
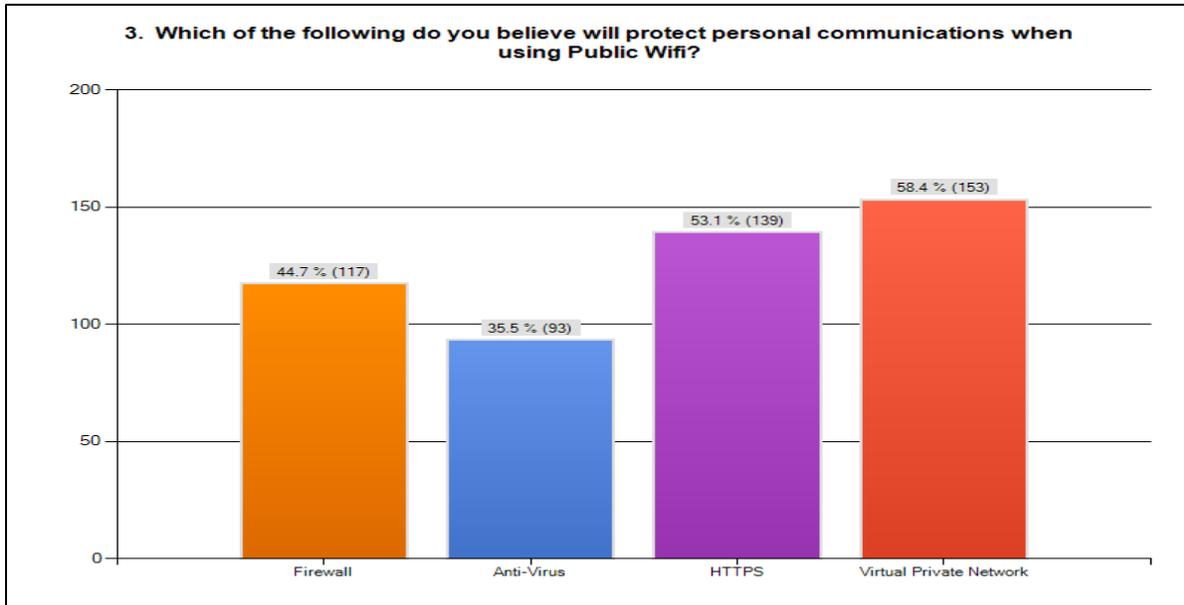
Survey Results:

Question 1, which asks the survey participant about their own use of public wireless Internet connections (public WiFi), had 377 initial respondents, of which 82 responded they did not use public WiFi. Of the remaining 295 respondents, approximately 270 answered the remaining questions. Although 22% did not use public WiFi, 78% used public WiFi connections at least once a month, and 41% used these connections at least once a week. It can be noted, of those who do use public WiFi (295 respondents) more than half (53%) use public WiFi at least once a week. (n=377)
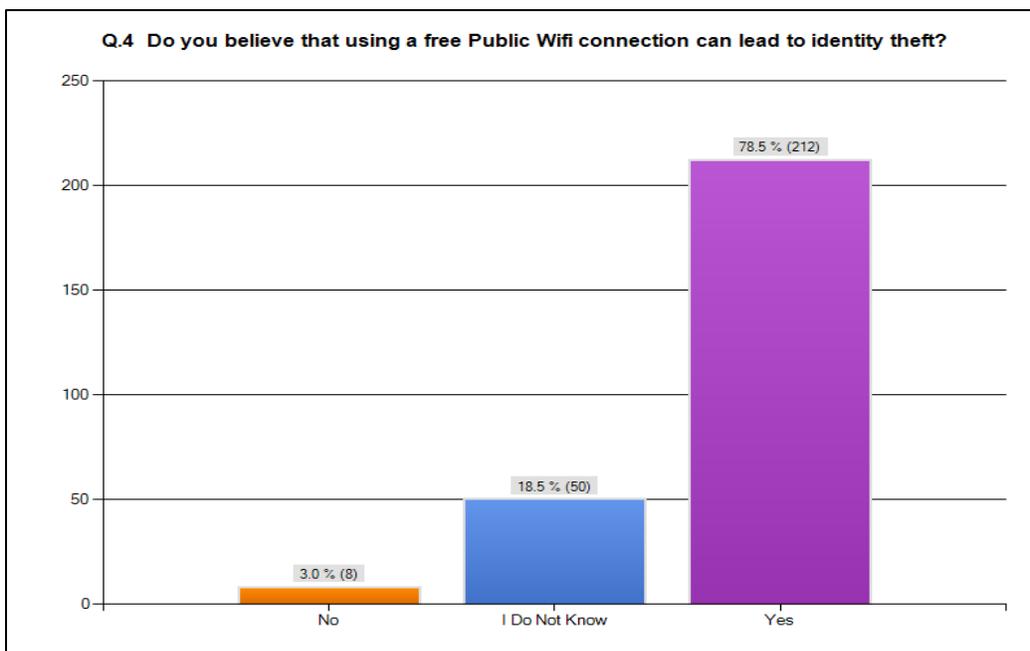
Q. 1 How often do you use a Public Wireless Internet Connection (Public Wifi)?

Category	Value
Everyday	64
Once a Week	92
Once a Month	139
I Do Not Use Public Wifi	82

Question 2 addressed the types of locations that consumers found it convenient to use a public WiFi connection over the course of the past 12 months. Not too surprisingly, coffee shops and restaurants were the most used, with approximately 3 out of 4 respondents choosing that category. Although usage at schools was the lowest, it must be remembered that this is a survey of the general population, and students would be a subset of the surveyed population. Over half the respondents used hotel WiFi services, and about 4 of 10 connected at the airport. The "other" category contained a large number of different locations including doctor's offices, hospitals, malls and retail outlets, public transportation and city/government "hot spots." (n=276)

Q.2 In which of the following places have you used Public Wifi in the past 12 months?

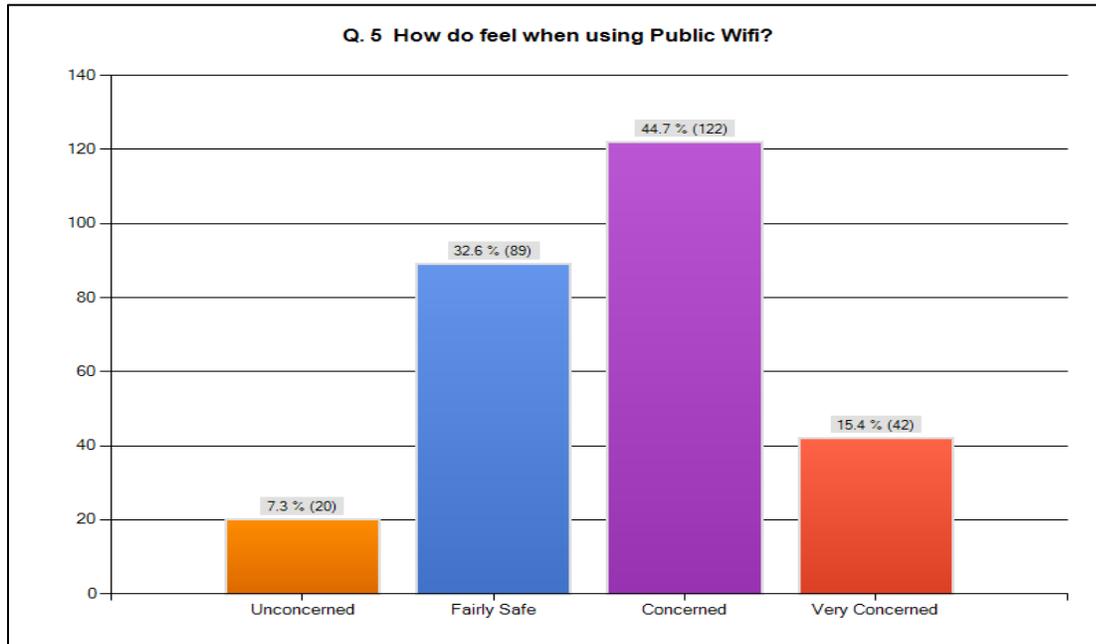| Location	Percent (count)
Airport	38.4 % (106)
Hotel	54.3 % (150)
Library	26.4 % (73)
School	21.0 % (58)
Coffee Shop / Restaurant	73.6 % (203)
Other, please specify	26.1 % (72)

Question 3 explored consumer perception as to what well-publicized safety tools would have an impact on protecting them while using public WiFi connections. ITRC noted that this question resulted in slightly fewer responses than the average response to other questions on this survey, possibly because some did not feel comfortable with technology based questions. Firewalls, anti-virus, and use of HTTPS connections, especially when used correctly together, can provide significant protection of personal communications while using public WiFi. The responses reflect some understanding of their merit. It is encouraging that 58% recognize that virtual private networks (VPN's) are an important method of protecting public WiFi personal communications content. (n=262)
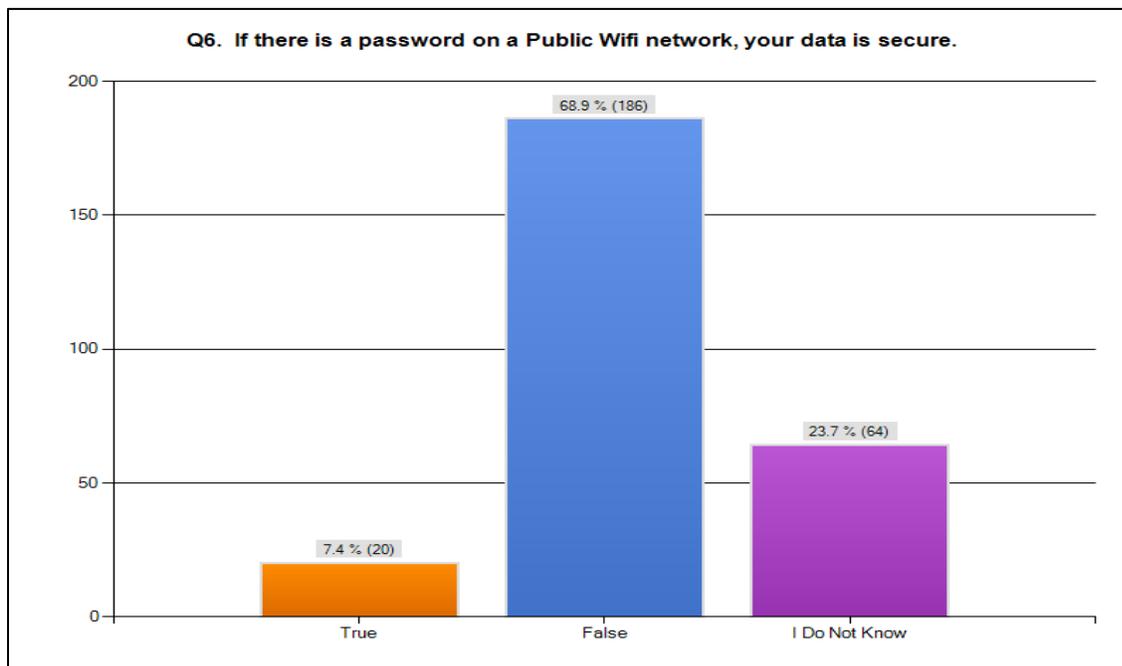

3. Which of the following do you believe will protect personal communications when using Public Wifi?

- Firewall: 44.7 % (117)
- Anti-Virus: 35.5 % (93)
- HTTPS: 53.1 % (139)
- Virtual Private Network: 58.4 % (153)

Question 4 indicated that almost 4 out of 5 respondents understood that using a free public WiFi could make them vulnerable to identity theft. Unfortunately, nearly 1 out of 5 did not recognize the potential threat posed by public WiFi. (n=270)


Q.4 Do you believe that using a free Public Wifi connection can lead to identity theft?

- No: 3.0 % (8)
- I Do Not Know: 18.5 % (50)
- Yes: 78.5 % (212)

Question 5 asked "how do you feel about using Public WiFi?" 40% of the respondents indicated no concern, or felt fairly safe. The remaining 60% felt concerned or very concerned. While it is positive that the majority seem to be aware of the risks of using a public WiFi connection, unfortunately, there appears to be a significant population that does not know about the risks, or does not feel it will happen to them. (n=273)

Q. 5 How do feel when using Public Wifi?

Unconcerned	7.3 % (20)
Fairly Safe	32.6 % (89)
Concerned	44.7 % (122)
Very Concerned	15.4 % (42)

Question 6 attempted to determine if the average public WiFi user understood whether their data is secure while logged into a network that required a password. A large majority, 7 out of 10, recognized that a password protected public network does not make your data secure. It is important for consumers to know that other users, who are also logged into the same public WiFi network, are in an excellent position to "sniff" your data, and perhaps directly attack your laptop or device. (n=270)

Q6. If there is a password on a Public Wifi network, your data is secure.

|	
True	7.4 % (20)
False	68.9 % (186)
I Do Not Know	23.7 % (64)

Question 7 found that 44% of survey respondents did not know, or did not believe, that there are ways to protect sensitive data while using public WiFi. However, a larger percentage of respondents (56%) answered that there are ways to protect sensitive data when using public WiFi. It should be noted that the method of protection is not defined in this question. (n=273)
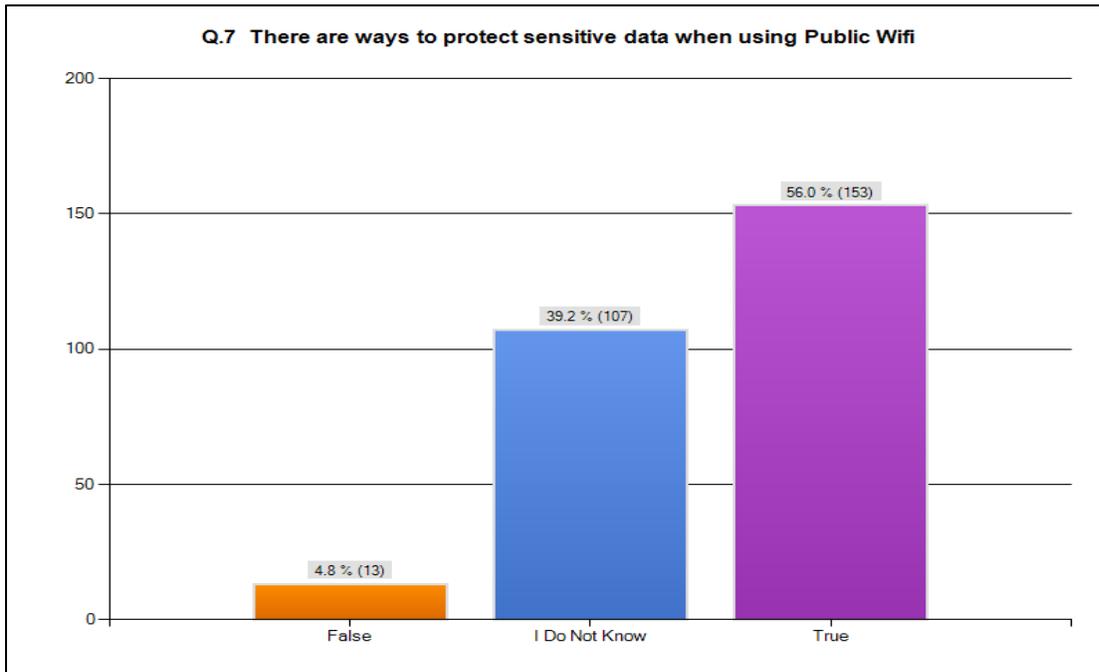
Question 8 sought to understand what part of the public WiFi user population logs into work or business related resources while using a public WiFi connection. As indicated by the participant responses below, 57% had accessed work resources while using a public WiFi connection. Unfortunately, we do not know whether or not a VPN, personal or corporate, is being used for these work connections. (n=270)
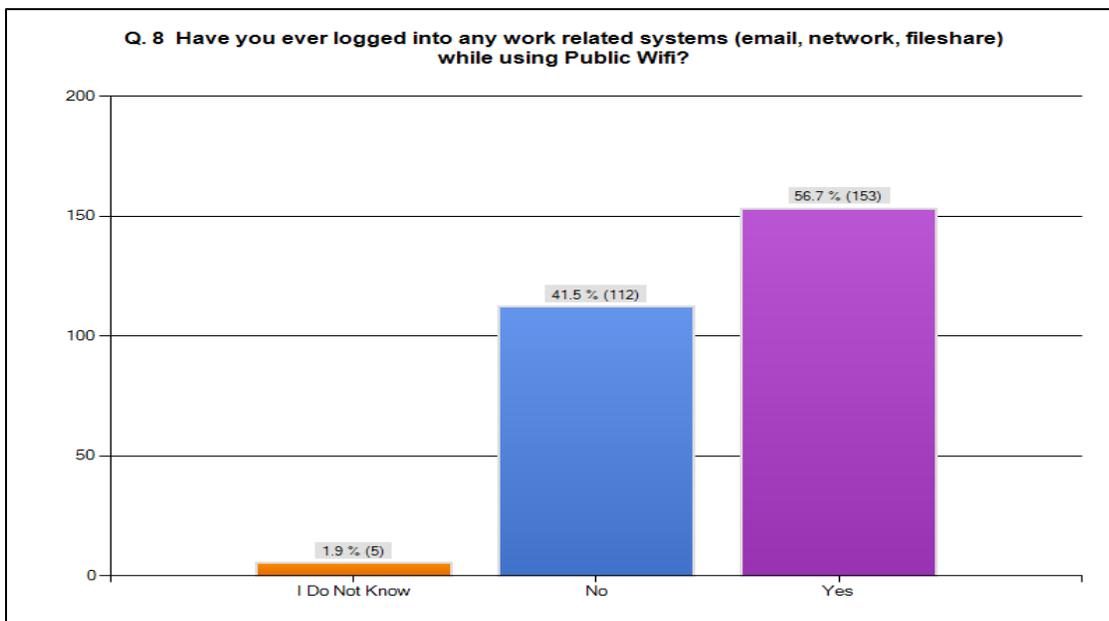
Question 9 surprisingly indicates that 1 in 4 of those using public WiFi connections have made a purchase using a credit card on those connections. The 24% who acknowledged making purchases on public connections unknowingly exposed themselves to having their credit card information made available to other users on the public WiFi network. ITRC is quite frankly skeptical that 72% of the survey takers have never made a purchase while using a public WiFi. Many of those may have made a credit card purchase just to access the WiFi network. (n=272)
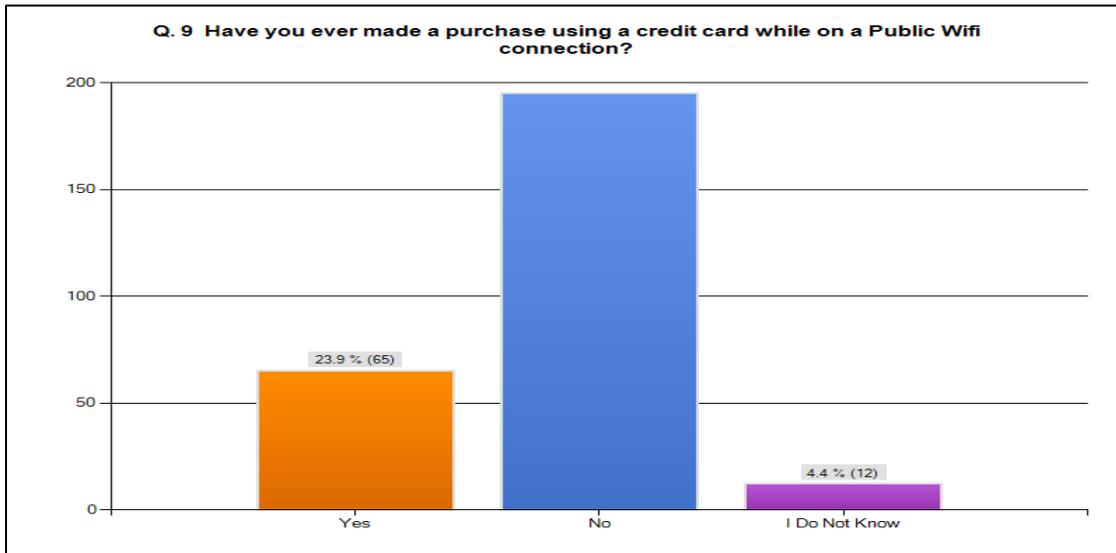
In **Question 10**, when asked whether or not they currently use a VPN, 27% of the respondents answered that they do, while 73% indicated that they did not (or they did not know). The responses to this question clearly reflects the need for further investigation. For instance, if only 27% of respondents use a VPN, but 57% have logged into work related systems while using public WiFi, what accounts for the large discrepancy (30%) between those who **know** they are using a VPN, and those who most certainly **should be** using a VPN? (n=273)