Rolling the Dice with Public Wi-Fi

A Xirrus Wi-Fi User Survey Report | October 2016

DON’T PLAY GAMES. KNOW THE RISKS.

91%
SAY PUBLIC WI-FI IS NOT SECURE

89%
USE IT ANYWAY
Introduction

Wi-Fi has enabled the mass adoption, use and innovation of connected devices. With connectivity creeping into almost every aspect of our lives, we’ve come to expect public Wi-Fi at nearly every place we go. Wi-Fi is no longer a want, but a need. Still, very few networks are capable of protecting our data when we connect. Simply put, the networks don’t encrypt data (among other things), leaving a myriad of security risks.

The average total cost of a breach is $4 million, which is up 29 percent since 2013. Concern continues to grow around the insecurity of public Wi-Fi networks, especially with the associated threats they pose to user devices and confidential user data. Now more than ever, large and small organizations — from coffee houses to airports and hotels — must upgrade their networks to provide better security for their customers. Moreover, as the workforce becomes increasingly remote and nomadic, businesses are responsible for ensuring employees have the tools and education to keep data safe. In many cases, there’s no longer an option to avoid working outside of the office or home. You may need to send a presentation to colleagues before jetting off on a flight, or access work applications from a coffee shop while on vacation. But are employees truly being safeguarded by businesses that offer public Wi-Fi?

In a 2015 Xirrus report, Where the Wires End, most respondents (79 percent) stated that they don’t feel that public Wi-Fi is secure; however, the majority (62 percent) still use it. One year later, Xirrus’ new research details trends in public Wi-Fi usage, the risks associates with connecting to these public networks and the impact of potential Wi-Fi data breaches. The following is a look at the industry’s take on public Wi-Fi and users perception of risk.

FINDINGS AT A GLANCE

- 48 percent of Wi-Fi users connect to public Wi-Fi at least three times per week; 31 percent connect to public Wi-Fi every day.
- 91 percent of Wi-Fi users do not believe public Wi-Fi is secure, yet 89 percent of Wi-Fi users choose to use it anyways.
- On public Wi-Fi, 83 percent of Wi-Fi users are accessing their email, whether it’s for work or personal reasons, and 43 percent are accessing work/job specific information.
- Nearly half (46 percent) of Wi-Fi users say their company has not offered cyber security training in the past year.
Methodology
In June 2016, Xirrus, in conjunction with Morgan Wright, internationally recognized expert on cybersecurity and senior fellow at The Center for Digital Government, set out to discover how and where people connect to public Wi-Fi, user’s perception of risk and what educational measures organizations are putting in place for security.

Xirrus surveyed more than 2,000 executives and IT professionals in the U.S. to better understand their perception of public Wi-Fi networks.

Survey respondents came from a variety of industries including technology, education, finance and healthcare.

We Are a Mobile Society
Public Wi-Fi is available and users connect, nearly everywhere
As a mobile society, we are dependent on finding a network connection. While nearly all Wi-Fi users regularly connect to Wi-Fi in their homes, a vast majority of Wi-Fi users also connect to public Wi-Fi outside of their home. To break it down, 83 percent connect to Wi-Fi at hotels, 72 percent connect at coffee shops and restaurants, 64 percent connect at airports, 48 percent connect in co-working spaces and 41 percent connect convention centers. We access Wi-Fi anywhere we can, whether it’s for work or for leisure, which puts both business applications and personal applications at risk. We are always on the go, so Wi-Fi users are more than likely outside of their own “secure” environment at work or home. This creates more opportunities for threats to succeed.

Where do you connect to public Wi-Fi?

How often do you connect to public Wi-Fi?

48 PERCENT OF WI-FI USERS CONNECT TO PUBLIC WI-FI AT LEAST THREE TIMES PER WEEK; 31 PERCENT CONNECT TO PUBLIC WI-FI EVERY DAY

Mobility is no longer a want, but a need. Home networks are a given, but now people need connectivity everywhere they go and at all times. A growing number of users connect to public Wi-Fi networks at least three times per week if not every day.

Number of networks used daily

44 PERCENT OF WI-FI USERS CONNECT TO THREE OR MORE NETWORKS PER DAY

The home and work Wi-Fi networks are the two most prevalent Wi-Fi networks people connect to on a daily basis. Because they are private and only a select amount of users gain access, these are the safest networks to join. The third network presents the biggest problem. The more networks a user connects
to, the more likely he/she is to download malware on a public connection (i.e. coffee shop) and bring the virus into a secure network (i.e. home or work).

70 PERCENT OF WI-FI USERS WOULD CHANGE THEIR HOTEL FOR IMPROVED WI-FI SECURITY AND PERFORMANCE, WITH COFFEE SHOPS AND RESTAURANTS IN CLOSE SECOND (68 PERCENT)

In 2015, more than half (66 percent) of Wi-Fi users said they would change hotels for a better Wi-Fi experience. That number increased this year. Increasingly, travelers not only expect faster, more reliable Wi-Fi, but also security built in. People have realized performance is no longer enough on its own; it goes best with security. The report found that respondents would book travel accommodations elsewhere if there was “bad” or “insecure” Wi-Fi.

Are We Secure?

91 PERCENT OF WI-FI USERS DO NOT BELIEVE PUBLIC WI-FI IS SECURE, YET 89 PERCENT OF WI-FI USERS CHOOSE TO USE IT ANYWAYS

In 2015, most users (79 percent) stated that they don’t feel that public Wi-Fi is secure; however, the majority (62 percent) still use it. In 2016, 91 percent of the sampled population don’t believe public Wi-Fi is secure, while 89 percent choose to still use it. While more Wi-Fi users are aware of the risk, an increasing number of Wi-Fi users connect anyways.

Whether it’s online banking or work email, Wi-Fi users are accessing sensitive information over public Wi-Fi

Multitasking and accessing information, no matter the location, has become commonplace. Wi-Fi needs to have the security and performance to sustain the many different activities and applications employees are engaging in and with daily. 83 percent of Wi-Fi users are accessing their email, whether it’s for work or personal reasons and 43 percent are accessing work/job specific information. 42 percent of Wi-Fi users are shopping and 18 percent are logging into banking applications on public Wi-Fi. These two activities specifically expose more personal information to potential intruders. No matter what application users are accessing, personal and business critical data is exposed to potential threats.

Ransomware is the least known cyber threat by Wi-Fi users

Wi-Fi users are aware of most cyber threats. But ransomware is the least known, despite its prevalence, evolution and danger. This leaves not only businesses but also individuals vulnerable to attack. And yet, nearly 30 percent of respondents are unfamiliar with ransomware. Organizations and users are increasingly
being targeted by ransomware and more often than not pay the ransom to regain control of their data. New research from Symantec reveals that infection numbers jumped to 56,000 in March 2016, roughly double the normal rate, and the average ransom demanded by attackers more than doubled, as it rose to $679 (from $294) at the end of 2015. Cyber security expert and Senior Fellow at The Center for Digital Government, Morgan Wright states, “As ransomware gets more sophisticated, the number of victims and methods of attacks will only increase. Businesses not only have a corporate responsibility to educate their users of the risks associated with connecting to public Wi-Fi, but also to give them the necessary tools to avoid attack.”

Nearly half (46 percent) of Wi-Fi users say their company has not offered cyber security training in the past year

39 percent said their employers have offered 1-2 trainings in the past year. With the cybersecurity threat landscape becoming increasingly complex, employees who practice unsafe cybersecurity habits put both themselves and their employer at risk. Working with Human Resources, it is up to the organizations’ CIOs, CISOs and IT leaders to put into practice regular cyber security trainings for its employees, so they are not only aware of the risks out there, but also how to avoid them.

There is a large gap between employers who encourage security when traveling, and those that do not

Majority (47 percent) say their employers encourage them to use a VPN when traveling for business. But a shocking 26 percent say their employers don’t recommend any security measures when traveling. The risk is clear.

Wi-Fi users blame themselves more often than not if they get hacked

85 percent of Wi-Fi users would blame themselves if they get hacked, only 32 percent would blame the Wi-Fi vendor and 24 percent would blame the venue. Most businesses do not equip their employees with the information and tools to stay vigilant and safe. Because of this, Wi-Fi users carry the burden of corporate mismanagement.
Security Measures Encouraged

- Use a VPN: 47%
- Two-factor Authentication: 17%
- None: 26%
- Don’t connect to public Wi-Fi: 10%

Conclusion

Today’s people expect public Wi-Fi at nearly every place they go — coffee shops, airports, hotels or on a plane. 48 percent of Wi-Fi users connect to public Wi-Fi at least three times per week; 31 percent connect to public Wi-Fi every day. But even with public Wi-Fi use increasing rapidly, very few Wi-Fi networks meet our security needs when we leave home. Though accessible and convenient, typically they don’t encrypt data, which leaves passwords exposed and sensitive data vulnerable to the possibility of capture by nefarious predators.

People give plenty of thought to keeping physical possessions safe when stepping out of their home. They pack away jewelry, laptops and smartphones, or keep them close by. While these physical possessions stay top of mind for people, data on the other hand, does not draw the same attention.

Additionally, a vast majority of Wi-Fi users would blame themselves if they were to get hacked. While most Wi-Fi users are aware of the risks, they connect anyway without the necessary tools to stay safe. With more employees working from home or traveling for work, businesses are not equipping their employees with the information and tools to stay vigilant. In the past year, nearly half (46 percent) of Wi-Fi users say their company has not offered cyber security training. Because of this, Wi-Fi users carry the burden of corporate mismanagement.

Morgan Wright provides the following tips before connecting to public Wi-Fi:

- Update your security software and operating system
- Put a PIN or passcode on all your mobile devices
- Get identity theft protection with comprehensive restoration
- Encrypt all of your data
- Carry the security of your personal network everywhere you go

Secure personal networks via a simple, one-time process that authenticates all devices, ensure the data across Wi-Fi users’ platforms is safe inside the public network at all times. Unlike a VPN, which encrypts end-to-end connections back to a corporate network and requires additional software, a user can easily create their own secure personal network that automatically encrypts the data on the Wi-Fi network.

Regardless of concerns around public Wi-Fi and the security risk, people continue to use it. The need to connect supersedes security implications. Additionally, employers are not stressing the importance of staying vigilant while outside of the secure corporate or home network, which is problematic. As illustrated by this research, much remains to be done to change this mindset among Wi-Fi users and enterprises alike.