Private WiFi

WHITEPAPER: OCTOBER 2014

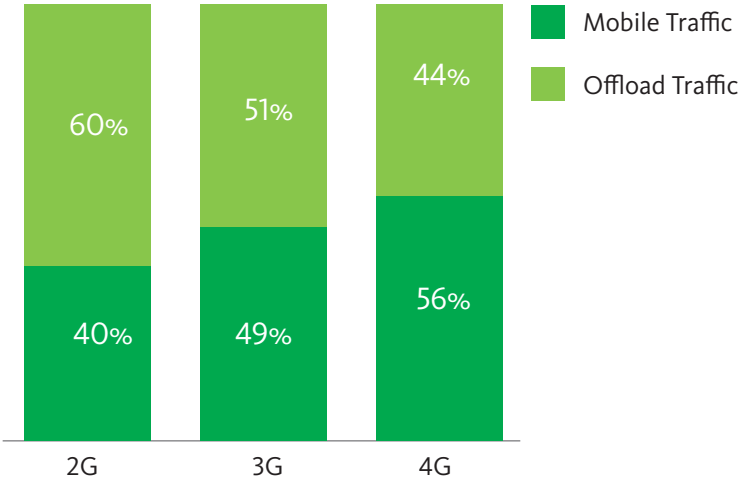
The Hidden Dangers of Public WiFi

Private WiFi

EXECUTIVE SUMMARY

By the end of 2014, the number of mobile-connected devices will exceed the world's population, according to Cisco's Global Mobile Data Traffic Forecast Update. Further, Cisco predicts that by 2018 there will be more mobile traffic on WiFi than cellular networks. As the graphic indicates, this is especially true for more advanced data network standards like 3G, 4G, and LTE.

Mobile and Offload Traffic from Mobile-Connected Devices



Source: Cisco VNI Mobile, 2014

ABI Research predicts that WiFi hotspots will reach 7.1 million in 2015, coinciding with the increase in mobile-connected devices. According to JiWire Mobile Audience Insights Report Q4 2013, WiFi usage on smartphones and tablets has increased 16% year over year, with 67% of connections occurring on a mobile device.

People are using WiFi hotspots because the technology is often accessible at little or no cost. In fact, according to a 2013 survey by The Identity Theft Resource Center (ITRC), U.S. consumers are three times more likely to connect to a WiFi network if it is free. The ITRC calls this trend "The Convenience Factor" likely due to the fact that WiFi hotspots are available in many public places, allowing users to get and stay connected, wherever they are.

Private WiFi

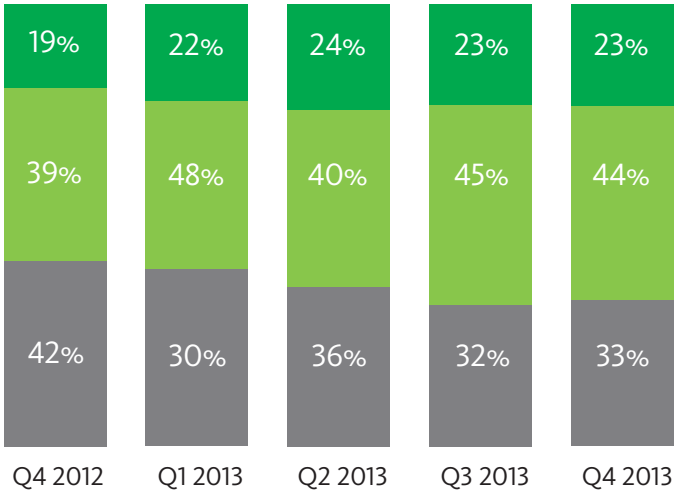
While constant connectivity simplifies online activities, the rise of mobile devices and the global proliferation of WiFi networks can be a dangerous coupling. In fact, many WiFi hotspot users are unaware of the hidden risks that the technology poses—such as identity theft, hacking, and compromised bank accounts.

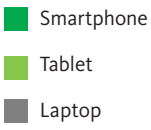
This whitepaper aims to educate people and businesses on what they need to consider before connecting to WiFi. Also, the report will explain how this technology can be detrimental to users and what people and the businesses that service them can do to protect WiFi users from the inherent threats that hotspots pose. The report offers information about security and privacy options available in the market today, such as a Virtual Private Network (VPN), which guarantees users that their privacy and security will remain intact.

...many WiFi hotspot users are unaware of the hidden risks that the technology poses—such as identity theft, hacking, and compromised bank accounts.

Connected Device Trends: Public WiFi Usage

How are Consumers Connecting to WiFi?





Mobile devices grew from 58% to 67% of Wi-Fi connections year over year, a 16% lift

› 67% of all public Wi-Fi usage was represented by mobile devices, with smartphones at 44% & tablets at 23%.

› Laptop usage decreased to 33% of usage, a relative decrease of 21% year over year.

› In Q4 2013, mobile Wi-Fi connections plateaued.

MARKET DYNAMICS

The Promise of Public WiFi

WiFi is convenient, accessible, and operates in millions of homes, corporate offices, university campuses and public hotspots worldwide. WiFi networks use radio waves, similar to cell phones and televisions, to connect to a wireless access point called a router, which directly connects to the Internet via a cable or DSL modem.

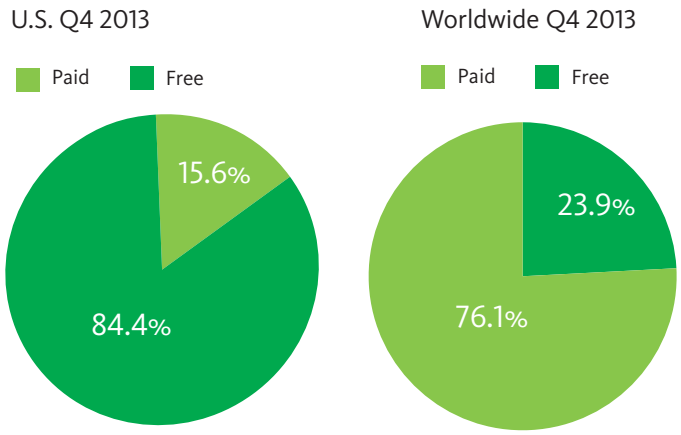
Users recently connecting to WiFi at an airport, coffee shop, library, park, or hotel have all used an open WiFi network. Locations with open and public wireless access are called wireless hotspots. Any user—even hackers—within 300 feet of the access point can then access the network.

According to a Harris Poll survey conducted on behalf of PRIVATE WiFi in March 2014, 66% of U.S. adults have used public WiFi. This means the majority of adults in America are getting and staying connected all over the country.

U.S. consumers are three times more likely to connect to a WiFi network if it is free.

As the below graphic from JiWire's Mobile Audience Insights Report Q4 2013 illustrates, nearly 85% of U.S. public WiFi hotspots are free. Worldwide, the U.S. also saw the most growth in free WiFi with close to a 6% increase in the number of public wireless connections.

Public WiFi Business Models



The Problem with Public WiFi

However, most WiFi hotspot users are not aware of the inherent threats: public WiFi networks are almost always unencrypted, which means that anyone with cheap, easily available software can listen in and access everything being sent over the network.

The following hacks can occur while accessing public WiFi hotspots:

Sniffers: Software sniffers allow hackers to passively intercept data sent between a web browser and web servers on the Internet. Hackers can capture any email, web search, or file transferred on an unsecured network.

Evil Twin: An evil twin is a rogue WiFi access point that appears to be legitimate but actually has been set up by a hacker to fool wireless users into connecting a laptop or mobile phone to a tainted hotspot. Once the victim connects to the evil twin, the hacker can listen to all Internet traffic or even ask for credit card information posing as a standard pay-for-access deal.

Man-in-the-Middle Attacks: Any device that lies between a user and a network server can execute man-in-the-middle attacks, which intercept and modify data exchanged between the user and the server.

Sidejacking: Sidejacking is a method where an attacker uses a packet sniffer, a program that can intercept or log traffic passing over a digital network, to steal a session cookie containing usernames and passwords from a variety of websites, such as Facebook or LinkedIn.

...wireless eavesdropping can happen on virtually any public WiFi network.

Many users assume that if they pay for an open WiFi network at a hotel or airport then that connection is as secure as the network connection at home or at the office. But wireless eavesdropping can happen on virtually any public WiFi network. Plus, it is impossible for the untrained person to determine the safety of a public WiFi network and to identify those that are dangerous and make users vulnerable to hacking. Unfortunately today, the onus is on WiFi users to protect themselves from such threats.

Private WiFi

MARKET BEHAVIOR

Most People Do Not Protect Themselves While on Public WiFi

Most U.S. adults are unaware of the threats on public WiFi networks, or they are aware of them but choose not to protect themselves. According to the aforementioned Harris poll, 39% of U.S. adults have accessed or transmitted sensitive information while on public WiFi without taking any steps to protect their data.

When asked in what ways they have accessed sensitive information while using public WiFi:

26% say they have checked a bank account

19% say they have paid a bill

8% say they have sent an email with sensitive information such as their Social Security number or an account number

6% say they have filed their taxes

10% say they have done so in another way

Also, the survey revealed U.S. adults' attitudes toward potential threats when accessing free public WiFi.

When asked about potential issues with using free public WiFi when accessing or transmitting confidential information:

88% of U.S. adults mentioned identity theft

76% answered compromised accounts

39% noted that fraudulent tax filings could be a potential issue

This survey proves that even though people are afraid of the potential threats that public WiFi poses, many still perform activities that could make them vulnerable to identity theft.

Thwarting Security Threats

The risks of public WiFi are inherent, but there are security methods that can be employed to thwart the threats. The problem is improper knowledge on which forms of protection actually work. Antivirus software, firewalls and HTTPS each play their own role in online security, but a virtual private network (VPN) is the only technology that fully addresses all the problems that public WiFi poses.

Antivirus and Firewalls: Not Enough

While antivirus and firewalls are essential tools for online safety, unfortunately they do not protect the users from hackers on a shared network, whether in a public hotspot (parks, cafes) or open WiFi network (hotels, airports). Antivirus software locates and deletes computer viruses, computer worms, Trojan horses, spyware, and adware from your computer. Firewalls are software programs that control the flow of traffic to and from the connected computer and either permit or deny communications. Both are necessary to thwart other cyber attacks, but will not safeguard data transmitted on an open wireless connection.

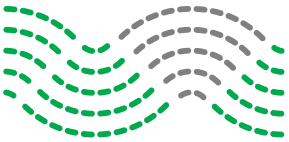
HTTPS and Its Limitations

Secure websites can help protect people from the dangers of WiFi hotspots, but the technology is no longer sufficient to ensure a user's privacy. Retailers, banks, and a variety of companies use secure websites — HTTPS (Hypertext Transfer Protocol Secure) — to provide secure transactions. The user can tell whether a website is "secure" if vit has "https" in the

Antivirus and firewalls... do not protect the users from hackers on a shared network.

URL and features a small lock symbol. SSL, or Secure Sockets Layer, is the technology behind HTTPS. TLS, or transport layer security, is the successor to SSL. Both technologies create an encrypted link between a website and the connected device's browser and ensures that all data passed between them remains private.

Up until now, most consumers were advised to rely upon HTTPS for protected online transactions, but it's possible for hackers to create fake websites that look very much like the real thing and SSL certificates can be forged or stolen. These faked or stolen SSL certificates can then be installed on fake websites in order to perform man-in-the-middle attacks or to attach malware to a visitor's computer. Due to these vulnerabilities, it would be a mistake to assume that secure websites are foolproof in terms of safeguarding personal information on public WiFi.



THE SOLUTION TO THE DANGERS OF PUBLIC WIFI'S INSECURITY

A Personal VPN

Fortunately, a solution is available. Just as people already rely on antivirus and firewalls, a VPN (virtual private network) could be considered the third leg of protection – perhaps the most important leg of all. A VPN fully addresses all the problems that public WiFi poses and protects users when they access public WiFi on their computer or mobile device.

A VPN encrypts all the data going into and out of the consumer's computer or mobile device, and the two sides use the same encryption algorithm and key. This technology blocks hackers from attempting to intercept or change data communications whether they utilize software sniffers, set up an evil twin hotspot or attempt a man-in-the-middle attack.

A VPN fully addresses all the problems that public WiFi poses and protects users when they access public WiFi on their computer or mobile device.

Without a personal VPN, users have no control over who can see their data as it crosses an open WiFi network. As data is being sent from a WiFi router to a computer or mobile device over radio waves, the hackers can intercept or hijack the data.

According to the aforementioned Harris study, 45% of U.S. adults who don't already use a VPN would purchase a subscription if it was affordable, and 24% said they would purchase a subscription if their identity were compromised. Luckily, VPNs are both affordable and easy to use.

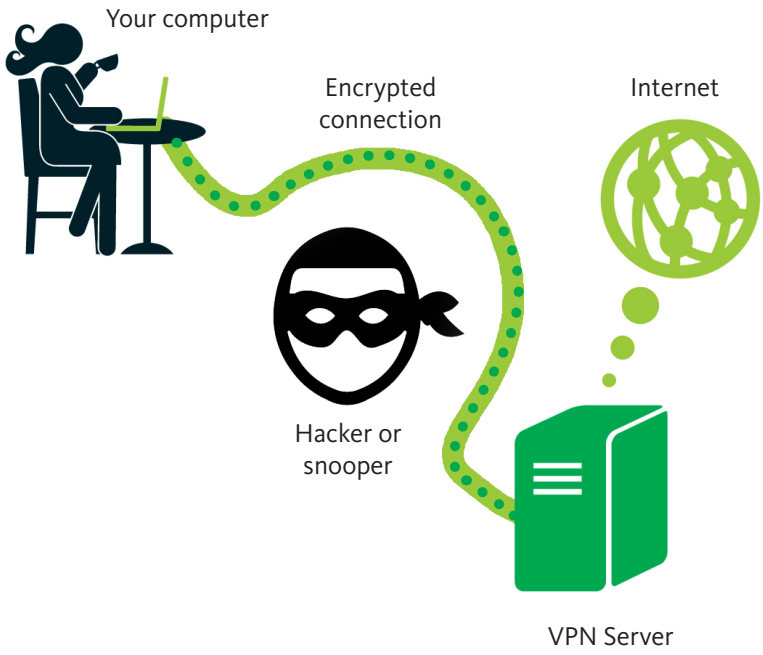
A personal VPN like PRIVATE WiFi offers a great solution to help WiFi hotspot users stay secure. The technology is a small piece of software that automatically encrypts and decrypts all data being transmitted over the radio waves rendering WiFi users and their data invisible to hackers.

Private WiFi

Guaranteed Security on WiFi

Employing a personal VPN is the only way for WiFi users to ensure their privacy and security when connected to a public hotspot. For all types of users – from the small business owner to road warriors to freelancers at a local coffee shop – there is no easier way to protect the data they send and receive. Making all sensitive and personal information encrypted and safe from cybercriminals, a VPN is a guaranteed way to prevent identity theft, compromised accounts, and exposed credentials.

How a Personal VPN Works



Private WiFi

SOURCES

76% Say Free WiFi Can Lead to Identity Theft [INFOGRAPHIC]: Identity Theft Resource Center and PRIVATE WiFi, November 12, 2013

Are You Protected From Hackers on Public WiFi? [INFOGRAPHIC]: Harris Poll on behalf of PRIVATE WiFi, April 3, 2014

Global Mobile Data Traffic Forecast Update, 2013–2018: Cisco, February 5, 2014

Global Wi-Fi Hotspots Will Grow to 7.1 Million in 2015 as a Method to Offload Traffic: ABI Research, May 8, 2014

Mobile Audience Insights Report: JiWire, Q4 2013

ABOUT PRIVATE WIFI

PRIVATE WiFi is a product of Private Communications Corporation, which is dedicated to protecting individual privacy and corporate data security online.

If you are interested in learning more about PRIVATE WiFi and its VPN technology, contact info@privatewifi.com.