Journal of Forensic & Investigative Accounting
Vol. 5, Issue 2, July - December, 2013

# Wi-Fi Hotspots: Secure or Ripe for Fraud?

**Richard G. Brody***
**Kyle Gonzales**
**Dustin Oldham**

In today's society, Wi-Fi has become one of the most popular ways to access the Internet. Organizations have implemented "Free public Wi-Fi" to attract consumers, and increase the duration of time the consumer will spend within the business. According to Aroon (2010), "As of March 22, 2010 there were 296,732 free and pay Wi-Fi locations in 145 countries… [t]he United States leads the world with 72,156 hot spots" (para. 2). The most common places that utilize these hotspots are coffee shops, airports, and hotels. The amount of traffic and lack of security inherent in public wireless hotspots creates a perfect environment for individuals to commit fraudulent activities. In fact, Potter (2006) states "[w]hen users use a wireless network, they give up a foundational piece of information security: the physical layer" (p. 54).

In order to explore this issue we will first examine why the data collected on unsecure wireless networks is such a large target for fraudsters and how the captured information is used to commit fraud. Next we will discuss the primary methods used to conduct attacks on public networks in order to harvest sensitive information. Finally, we will address the mitigating practices that individuals can implement to ensure privacy and reduce their risk of becoming a victim of fraud.

*The authors are, respectively, Douglas Minge Brown Professor of Accounting, and Graduates of the Information Assurance Program at Anderson School of Management in University of New Mexico.

## Public Hotspot Fraudulent Activities

Due to the inherent vulnerabilities associated with unsecured public wireless networks, fraudsters can use deceptive techniques to commit fraud by collecting information from users that are connected to the wireless hotspot. There is a vast amount of sensitive user data such as login credentials, bank account information, and social security numbers that can be monitored and stored. The fraudster can then monitor users' internet activity to gain more sensitive data and leverage this information to commit fraud.

An issue that compounds the vulnerability of wireless networks is the tendency of individuals to use the same login credentials to access multiple accounts. Thus, once the fraudster has the credentials from one site, it can be applied to several sites the victim has been observed using. According to OnGuard Online (2011), "…a hacker could test your username and password to try to gain access to other websites, including sites that store your financial information" (para. 6). The fraudster can also use this information to try to gain access to sites that use HTTPS, such as online banking sites. Once the fraudster has acquired personal information from the victim, it can be used to conduct fraudulent activity including a wide variety of white collar crimes such as tampering or creating new bank accounts, making purchases with credit card information, and other forms of identity theft. In some situations, the fraudster may even sell the information to other fraudsters for personal gain.

## Wireless Vulnerabilities

Public wireless access points are extremely vulnerable to fraudsters for four main reasons: attacks can be conducted anonymously, encryption mechanisms used as a security measure are often outdated, Wi-Fi attacks are very difficult to detect, and the attacks are being executed by a complex network of skilled individuals. According to Gralla (2007), "[t]he hacker steals what he wants to or plants malware, such as zombie software, then leaves, and you have no way of tracking him down" (para. 7). These characteristics of internet activity and the fraudster make public hotspots a very attractive target for potential perpetrators of fraud.

Attacks on public wireless networks do not require any face-to-face interaction of the fraudster and the victim since the perpetrator is only required to be within range of the wireless network, which can be a very large area as in the case of an airport. Unsuspecting victims connect to a Wi-Fi hotspot and have no idea that a hacker is stealing their personal information. For example, the Better Business Bureau (BBB) in Charlotte, North Carolina recently received complaints from identity fraud victims who had been hacked after connecting to Wi-Fi hotspots at the Charlotte-Douglass Airport (Legnitto, 2012). The unsuspecting users were completely unaware that hackers had stolen any information from their laptops until they checked their bank and credit card accounts. Unfortunately, it is all too typical for Wi-Fi users to realize they are victims after the fact.

Encryption mechanisms such as WEP, WPA, and WPA2 are the basis for encrypting a wireless network to maintain security. Fleishman (n.d.) explained how encryption mechanisms are not secure by stating "WEP … was thoroughly broken. Some researchers claim to be able to recover a WEP key in under a minute" (para. 4). As technology advances, encryption mechanisms become obsolete requiring stronger encryption methods. For example, consider what happened in 2005 to TJX, the parent company of T.J. Maxx and Marshalls. Hackers gained access to the company's computer system and retrieved tens of millions of records, including some 100 million credit card numbers ("Hi-tech heist," 2009). TJX had a security system during the time of its break in, but it relied on WEP to encrypt customer data. Prior to the incident, a TJX vice president recognized that WEP was not a sufficient security measure and acknowledged to his bosses in an email: “We are still vulnerable with WEP as our security key. It must be a risk we are willing to take for the sake of saving money” (“High-tech heist,” 2009, para. 31). The security breach that occurred at TJX stores highlights the importance of utilizing the latest technology and the severe consequences that may result from relying on an obsolete encryption code.

Fraudsters also incur very little risk since these types of attacks are very difficult to detect using methods such as intrusion detection system (IDS) or intrusion prevention system (IPS). Difficulty of detection stems from the fact that attacks utilize a low level network protocol. According to a network traffic analysis study at a public restaurant conducted in Austin, Texas by Na and Rappaport (2004), “[w]eb browsing and P2P applications were the two most popular applications, with the majority of carried data using the HTTP protocol” (p. 2). Furthermore, all information that is transmitted through an unsecured public Wi-Fi network is sent in plain text. Since all information is easily readable, attackers easily gather information without decryption.

Perhaps the most dangerous aspect is the individuals committing these types of attacks. The profile of these fraudsters is rapidly shifting from disorganized individuals towards highly organized and structured software development teams. This is very concerning due to the knowledge base and coordination that this type of fraudster would possess. These organized teams have acquired the attention of the federal government, “[t]he FBI and other law enforcement agencies are confronting a wave of computer crime that is highly organized and hard to combat with traditional methods” (“FBI vows,” 2011, para. 1).

To demonstrate the invisible danger associated with Wi-Fi, consider what Dr. Amit Sinha, a Motorola Engineer and Wi-Fi detective, discovered as he sat in the parking lot of high-tech company located in Silicon Valley (O’Brien, 2010). Sinha opened his laptop and launched a

Wi-Fi detection program, and he quickly generated a list of over 250 Wi-Fi access points inside the company's building. Alarmingly, over half of the access points in the building had either no encryption or an outdated version that a hacker could easily crack, thus allowing Sinha to see the types of devices that people inside the building were using and the names of the networks they were connected to. Sinha's experiment demonstrates that even in the high-tech land of Silicon Valley, Wi-Fi vulnerabilities exist. People seem to log onto whatever Wi-Fi signal they can find without thinking twice and then proceed to share sensitive information, such as credit card numbers and passwords. Meanwhile, hackers sit back and wait for the opportunity to carry out an attack. Overall, companies and individuals are making it all too easy for hackers with their relaxed attitude toward wireless security.

## Types of Attacks

Attacks can be conducted using many different methods and are usually conducted in an inconspicuous manner. The first type of attack is a traditional method in which the fraudster targets the MAC address of the intended victim and diverts all transmissions through the malicious machine. One common example of this is the use of an SSL strip that can remove all security protocols and capture the victim's sensitive information such as user names and passwords. The second type is where the attacker creates a network in which the target connects to the internet through the attacker's connection. This is one of the most popular types of attacks, and is commonly known as connecting through a peer-to-peer connection. The third type of attack is when the attacker creates a fictitious website to collect personal information such as the user's log-in credentials and could potentially install malware. The fourth type of attack is when the malicious user installs software onto the victim's machine to distribute mass spam email to people in the victim's address book. The third and fourth types of attacks can be used in conjunction to gather information long after the victim has been infected while using the public hotspot. The fifth type of attack occurs when the attacker connects to an unsecured wireless Internet signal and proceeds to install a “sniffer program” to capture sensitive information, including credit and debit card numbers.

Each of these attacks will now be discussed in detail. See Table 1 for a summary of the give types of attacks.

### Man-in-the-Middle

Man-in-the-Middle attacks are the largest threat amongst public Wi-Fi hotspots and are initiated when one user requests a connection to the access point. An attacker can capture this information and forward the request to the access point. A key exchange between the client and access point is required for every connection to occur. The attacker must provide a different public key than provided by the victim, and relay the attacker’s key to the access point. The interaction between the victim and the access point can then be achieved through the malicious medium of data transmission. When this occurs, all information sent through the malicious machine can be stored, altered, or redirected to facilitate the attack.

When this type of attack is executed, network traffic sniffers such as WireShark can be used to harvest information from packet payloads that are being transmitted. The information that can be gathered using this type of software can help the attacker determine sites the user is visiting. This information will help the fraudster determine the end user’s normal internet behavioral patterns. These types of exploits allow the fraudster to obtain sensitive data about the users such as any communication services being used and bank account or email information.

Mozilla Firefox offers plug-ins that allows users with limited “hacking” knowledge to learn to conduct malicious attacks to gain information. This plug-in allows a user to hijack the sessions of those on the same network using services affiliated with social networking sites such as MySpace, Facebook, and Twitter.  Nazareno (2011) explains how accessing social networks in a public location can be exploited by the following, "Firesheep [a Mozilla plug-in] helps users capture a Wi-Fi user's "cookies", or internet history tracking data, and use those cookies to gain access to a user's sessions on email and social networking accounting" (para. 8).  This type of information gathering allows for a social engineering attack in which case the fraudster poses as the victim to collect information through manipulative tactics.

### Peer-to-Peer or Evil-Twin Attack

The peer-to-peer type attack occurs when the fraudster provides a fake hotspot to the victim.  In this situation, the attacker broadcasts a signal from his or her computer to lure victims to connect to the internet through the attacker's machine.  This exploit can be executed by displaying a fake or misleading MAC address, mimicking an access point (AP), or creating a rogue or "ad hoc" network.  Mimicking an AP is the most complex but successful way for fraudsters to perform this type of attack.  This is very similar to a Man-in-the-Middle attack, but the victim initiates the connection with the attacker.  The attacker is usually closer to the victim than the access point; therefore, a stronger signal is received on the victim's machine by the rogue network created by the attacker.  The fraudster's will also deceive the user by broadcasting an appropriate SSID corresponding to the establishment, such as Starbucks or T-Mobile.  This makes the fake hotspot appear legitimate and more appealing to the user since the strongest signal available is usually associated with achieving the best internet performance.  The victim is then provided access to the internet relayed through the fraudster's machine, allowing the perpetrator to harvest online activities and gain access to folders and files on the victims' machine.  All user traffic is passed through the fraudster's machine who then receives all information about the target’s activities.  Roth, Polak, Rieffel and Turner (2008) state that this type of attack is extremely attractive to fraudster’s since “…hackers gain full control over the clients’ network communication…” and “…the access point to which a user’s device binds does not identify itself in a fashion that can be verified reliably by the user ” (p. 220).

**Pharming**

Another method fraudsters use to commit fraud on public hotspots is by creating a malicious web page on a portable machine which runs a browser based exploit.  The fraudster’s web page may look very authentic due to the fact the “view source” of the legitimate page displays the code which contains the format to create the page, links contained within the page, and the links to all the graphics on the page.  After creating a replicated page, the fraudsters then redirects all traffic on the authentic public hotspot to his or her malicious page where a browser based exploit is run.  This transaction can install malware such as key loggers, trojans, or even gain access to a live command shell on the targets machine.  A user that accesses a log-in webpage while using a public hotspot should always examine the page and URL before entering any credentials since this technique is an easy way for attackers to gain log-in account information.

**Phishing**

Phishing is another method to commit fraud using public hotspots which is similar to pharming in that it utilizes malware to acquire sensitive information.  Symantec Corporation (n.d.), a world renowned anti-virus company, presents the following phishing vs. pharming analogy, “[p]hishers drop a couple lines in the water and wait to see who will take the bait. Pharmers are more like cybercriminals harvesting the internet at a scale larger than anything seen before” (para. 3).  This technique has the potential to turn the end users computer into a “spam spreading zombie", which will access the address book of the victim and deliver malicious email from a trusted legitimate address. Phifer (2010) states that, "[o]nce poisoned, clients can be redirected to phishing sites long after leaving the hotspot, even when connected to a wired enterprise network" (para. 11). The emails sent by this type of attack do not always request personal information, but can link the target to a fictitious website to acquire the personal information. This software is intentionally installed by the attacker on victims' machines, which utilizes their address books and bandwidth to spread the virus. Installation of the malicious software is not detected, but feedback from acquaintances who receive the "spam" email messages are usually quick to notify the victim of the attack.

### Wardriving

The example mentioned earlier in which Dr. Amit Sinha, a Motorola engineer, used a Wi-Fi detection program to locate unsecured access points inside a building is an example of wardriving. Specifically, this technique involves using a laptop computer to look for accessible wireless Internet signals. Once a vulnerable network is discovered, the hacker can install what is called a "sniffer program" to capture such sensitive information as credit and debit card numbers and then proceed to sell the data (Lush, 2009). What is purported as the biggest credit card hack of the decade was carried out using wardriving. Albert Gonzalez hacked 170 million credit card accounts by finding retailers' accessible wireless Internet signals and then installing "sniffer programs" to gain credit and debit card numbers (Lush 2009). Retailers involved include T.J. Maxx, Barnes & Noble, Sports Authority and Office Max.

## Targets for Wi-Fi Fraud

When a hacker wants to gain access to a Wi-Fi network using one of the aforementioned attacks, where does he or she carry out the attack? Public Wi-Fi hotspots in McDonalds, Starbucks, Panera Bread, airports and hotels are all vulnerable areas. Interestingly, cars are one of the newest targets for hackers. Cars have become an "epicenter of multimedia activity for consumers…[and] all the major automotive players are getting in the game, offering movies on integrated LCD screens, enabling passengers to surf the Web or simply allowing access to an address book" (Savitz & Giordano, 2011, para. 1). Unfortunately, Wi-Fi enabled cars also are vulnerable to increased security risks. As passengers transfer such information as phone numbers and email addresses from mobile devices to their cars, this information could very well be susceptible to hackers. To protect against hackers, carmakers need to ensure that "the consumer's data is encrypted using a highly secure encryption standard such as the Advanced Encryption Standard (AES)" (Savitz & Giordano, 2011, para. 6).

Smartphone fraud is another area of growing concern. While smartphones are convenient, allowing individuals to check email, conduct banking transactions and update Facebook while on-the-go, they also leave users vulnerable to cyber criminals who strive to steal sensitive personal information (Poturalski, 2012). McAfee, a worldwide security company, recently released its 2012 projections for the top threats facing smartphones and mobile banking attacks were included. To carry out a mobile banking attack, a hacker uses "Short Message Service (SMS) messages to gain account access and spyware that gains control of devices and sends costly premium-rate text messages" (Poturalski, 2012, para. 2). Smartphone fraud is all too easy for today's hackers because millions of Americans have Wi-Fi capability on their smartphones. With so many Wi-Fi enabled phones on the market, it is becoming increasingly difficult to insure the security of such devices because the networks and applications are characterized by "complete openness" (Poturalski, 2012).

One victim of smartphone fraud is Alison Smith. She was hacked at a Panera Bread location in Ohio after accessing a public Wi-Fi there. Smith was activating her iTunes account on her new iPhone when she was asked to provide her credit card number. She obliged and, ultimately, a $2,000 fraudulent charge was made on her card to a charity in India. Smith learned her lesson and says that she has her mobile Wi-Fi switched off all the time and that she no longer uses credit cards on her phone (Poturalski, 2012). Indeed, to remain safe, it is best not to perform sensitive activities on mobile devices, such as banking and making credit card purchases, at public Wi-Fi hot spots. As the saying goes, "if it's too good to be true, then it probably is." This is certainly the case for free public Wi-Fi.

Perhaps the biggest issue facing smartphones is the ease with which developers are able to create applications. All a hacker has to do is download a popular application, take it apart and add malicious stuff, and then put it under their own application name (Poturalski, 2012). Some companies, such as Apple, are beginning to review the legitimacy of applications before allowing them to be available for purchase on the market, and hopefully other companies will follow. For more detailed information on smartphone fraud, see Brody, Banward & Hawthorne (2011).

## Preventative Measures

A search using the phrase "How to hack Wi-Fi" generated over 58,000 videos on YouTube and over 34 million hits on Google. Still, a 2012 survey of American Internet users revealed that "64% of those who use unsecure wireless networks say they have little or no concern about using them" (Legnitto, 2012, para. 3). In addition, a 2011 survey conducted for the Wi-Fi Alliance revealed that "only18% of public Wi-Fi users reported that they use a VPN to encrypt their information when they're logged into hotspots" (Legnitto, 2012, para. 4). The good news is that individuals can take preventative measures to avoid becoming the victim of an attack while utilizing a public Wi-Fi hotspot. Wi-Fi in a public environment should not be trusted; therefore, the end user must ascertain which connections belong to the organization and are legitimate. This may involve asking the organization the name of their network. Users should examine the login page to determine the connection interface's integrity. If the website that has been accessed contains any clues, such as misspellings on the page or in the address bar, the user should cease and disconnect from the network.

If the organization offers a VPN or encrypted connection to the internet, information transmitted is secured and greatly increases the security of data transmission. Currently, most Wi-Fi signals are unencrypted, leaving anything an individual does online in coffee shops, hotels and airports in readable format and ready to be intercepted by others using the same network. If the user must connect to the internet through an "ad hoc" network they need to verify that the computer broadcasting the peer-to-peer signal is a known and trusted machine. Every user who connects to a public wireless connection should select the options to only connect to "Access point (infrastructure) networks only" and disable "always connect to preferred network" when configuring the computer, which will prevent the user from automatically connecting to a rogue peer-to-peer SSID. With automatic connections to wireless networks, the user might think that he or she has connected to the public wireless network when he or she has in all actuality picked up a wireless signal that was set up by a hacker (Taylor & McNeal, 2011).

Advice from OnGuard Online (2011) suggests the following: "[d]o not use the same password on different websites. It could give someone who gains access to one of your accounts access to many of your accounts" (para. 7). It is always best practice to have different login and passwords between different web-based accounts. If an account's login information is compromised, the attacker will not be able to access other sites using the same credentials.

The end user should only transmit sensitive information over an HTTPS connection, which is a secured version of HTTP.  Web browsers default to directing to an HTTP connection, so it is imperative to type the HTTPS prefix when accessing secure websites so the redirect cannot be exploited.  Every end user should ensure that the computer has updated security patches, anti-virus, and network interface card (NIC) firmware on the user's machine.  This is critical to prevent fraudsters from accessing or installing malicious spamming software on the user's machine when accessing a public hotspot.  Implementing these controls and following these practices will reduce the probability of users being scammed by a fraudster while using a public Wi-Fi hotspot.

## Liability Issues

The current trend is for companies to offer free Wi-Fi to its customers as a way to boost sales. Starbucks offers free Wi-Fi at nearly 7,000 U.S. locations, McDonalds offers it at more than 11,500 locations, and Panera Bread also has free Wi-Fi at its 1,565 locations. The technology and practice is still relatively new, so the courts have yet to provide any definitive answers regarding liability for businesses that opt to offer free Wi-Fi. For instance, can business owners be held liable for cybercrimes committed by an individual connected to the organization's network? What about for information stolen from a user because the network is unsecure? The Computer Fraud and Abuse Act (CFAA) forbids certain acts of unauthorized internet access. For example, the law makes it a criminal offense for a user to intentionally access a network without authorization to obtain sensitive information or with the intent to defraud (Computer Fraud and Abuse Act of 1986).  This unauthorized element is often difficult to prove when a cybercrime is committed by a user through a public Wi-Fi hotspot since access is open to the public ("Wi-Fi Hotspots and Liability Concerns," n.d., para. 3).

The best advice for a business that provides free Wi-Fi to its customers is to take the necessary steps to reduce potential liability. There are several ways to accomplish this task. One method could involve forming an agreement with the Internet Service Provider (ISP) in which liability for internet service or content remains with the ISP. More commonly, organizations may opt to require a user to click through a use agreement and disclaimer prior to gaining access to the Wi-Fi network. The use agreement and disclaimer should forewarn users that the wireless access is not secure and that the internet content is not regulated or controlled by the business ("Wi-Fi Hotspots and Liability Concerns," n.d., para. 13). One additional measure businesses might want to consider, depending on the area the Wi-Fi hotspot covers, is to have a controlled sign-in or password access system to increase security and protection for users ("Wi-Fi Hotspots and Liability Concerns," n.d., para. 14).

## Available Software to Protect Vulnerable Wi-Fi Networks

### Wireless Intrusion-Prevention Systems

While organizations have used intrusion-prevention systems (IPS) to protect their wired networks from hackers since the 1990s, it was not until recently that vendors began to release wireless IPS products (Lawton, 2010). These products were developed to cater to the dramatic increase in wireless networks over the years and to respond to the widespread threats associated with Wi-Fi usage. An increasing number of companies are starting to use wireless IPS products, and "Frost & Sullivan, a market research firm, estimates the WIPS market will grow from $150 million in 2007 to $572.5 million in 2014" (Lawton, 2010, p. 12). The appeal of an IPS is that it has the ability to stop intrusions in advance as opposed to alerting a user to a break-in that has already ensued. Wireless IPSs take the traditional IPS one step further. In addition to preventing intrusions into Wi-Fi networks, wireless IPSs put a stop to certain behaviors "such as unauthorized wireless communications from employee computers to external networks" (Lawton, 2010, p. 12).

As a hacker attempts to intercept communication, steal confidential information, or plant malware, how does a wireless IPS do its job? A wireless IPS server "analyzes data that up to 500 transceivers collect," and it uses behavioral analysis and pattern matching to determine whether an attack is under way (Lawton, 2010). In particular, a wireless IPS looks for unauthorized access points and also works with "libraries of known threats' traffic patterns" (Lawton, 2010). Considering all of its various capabilities, the future looks bright for the wireless IPS market. After all, businesses offering free Wi-Fi are at risk of having their systems hacked, much like retailers experienced in the past by relying on outdated WEP to encrypt sensitive customer data. If a hacker gains access to an organization's internal network, he or she could corrupt the entire system and collect customer data, including credit and debit card numbers. This is why organizations need to invest in technology to ensure that their network is protected. A wireless IPS is one option and will undoubtedly be a great resource for businesses to utilize as Wi-Fi vulnerabilities increase.

### Virtual Private Network (VPN)

A VPN is a technology that adds an additional layer of security to outside networks by encrypting online communications (Richmond, 2011). While organizations have long had access to VPN technology, such technology was not always available for individuals. The benefit of a VPN is that it turns readable information into an indecipherable jumble of nonsense. A hacker might still be able to intercept data on a VPN, but the information gained would be useless. Recently, VPN technology has become increasingly available to individuals. One company, Private Communications Corporation, specializes in protecting individual and corporate data and was created specifically to address the security vulnerabilities associated with connecting to a public Wi-Fi hotspot.

In March 2011, Private Communications Corporation introduced PrivateWiFi, a form of VPN technology available to individuals and small businesses. PrivateWiFi costs $9.95 a month or $84.95 a year, a small price to pay in order to be able to use the Internet privately, safely and anonymously (Richmond, 2011, para. 5).

## Conclusion

Using a public Wi-Fi hotspot makes the target susceptible to becoming the victim of an attack. According to a report from the Wireless Broadband Alliance, the number of Wi-Fi hotspots will increase 350% by 2015, bringing the total to five million hotspots worldwide (Legnitto, 2012, para. 6). Unless Wi-Fi users start taking the necessary precautions when connecting to an unsecure network, there will also be an increase in the number of victims. There are numerous preventative measures that an individual can take when connecting to a public Wi-Fi network. While accessing the internet in a public location, use caution to avoid connecting to a peer-to-peer internet connection. A good rule of thumb is to avoid connecting to any unfamiliar networks and to disable automatic connections to wireless networks. The connection may seem legitimate, but all information could be getting recorded by the malicious computer. The user must avoid transmitting any sensitive information while accessing a public Wi-Fi hotspot. It is always recommended to use a wired connection if one is accessible in the public location. It is also imperative that the computer connecting to the public Wi-Fi hotspot is equipped with up-to-date patches and anti-virus software. This will reduce the chance of another computer on the public network being able to access the victim’s machine. When connecting to a public Wi-Fi network, users should also consider using a VPN to encrypt all data transmitted over the internet in order to prevent hackers from intercepting data in readable format. Handling sensitive information while connected to a public hotspot is highly discouraged, but HTTPS websites are essential if transmitting sensitive information on a public network.

It is all too easy for a user to connect to an unsecured Wi-Fi hotspot. Available wireless networks appear and a user consciously decides to connect to one of them. A laptop will not warn a user that the network is not legitimate, that he or she has connected to a fake website, or that an attacker is hacking his or her computer. It is up to the user to make smart choices when connecting to an unsecure network. In addition, organizations offering free Wi-Fi to customers can take steps to provide greater protection for users by utilizing a VPN or requiring a password to gain access to the system. Forensic accountants have a role to play in the process as well. They can advise their client, whether an individual or an entire company, about the dangers of connecting to a public Wi-Fi hotspot and conducting business on an unsecured network. Furthermore, forensic accountants can educate clients about steps they should take to ensure that proper controls are in place to keep sensitive data safe.

Overall, individuals who access a public Wi-Fi hotspot should behave as if someone is monitoring their activities.  Every user should also consider that accessing a free public hotspot will not always be free, and should always follow these three steps when accessing a public Wi-Fi hotspot:  “Stop, Think, Connect.”

## References

Aroon, P. J. (2010, March 26). *How many wi-fi hot spots are there in the world?* Retrieved from http://blog.foreignpolicy.com/posts/2010/03/24/quiz_how_many_wi_fi_hot_spots_are_there_in_the_world

Brody, R., Banward, D., & Hawthorne, K. 2011. Corporate Smartphones in Danger! *Fraud Magazine,* 26(6), 19-23.

FBI vows more focus on 'cyber threats'. (2011, June 9). *Bloomberg News*. Retrieved from http://www.americanbanker.com/syndication/fbi-vows-focus-on-cyber-threats-1038651-1.html

Fleishman, G, (n.d.). *Battered, but not broken: Understanding the wpa crack*. Retreived from http://arstechnica.com/security/news/2008/11/wpa-cracked.ars

Gralla, P. (2007, January 19). Don't fall victim to the 'free wi-fi' scam. *Computerworld.* Retrieved from http://www.computerworld.com/s/article/9008399/Don_t_fall_victim_to_the_Free_Wi_Fi_scam

Hi-tech heist. (2009, February 11). *CBS News*. Retrieved from http://www.cbsnews.com/210018560_162-3530302.html

Lawton, G. (2010, May). Fighting intrusions into wireless networks. *Computer, 43*(5), 12-15.

Legnitto, J. (2012, June 1). *Fast, free and out of control: Why wifi users disconnect from wireless security risks at hotspots*. Retrieved from http://www.privatewifi.com/fast-free-and-out-of-control-why-wifi-users-disconnect-from-wireless-security-risks-at-hotspots/

Lush, T. (2009, August 20). Accused credit card hacker lived large in Miami. *USA Today*. Retrieved from http://www.usatoday.com/tech/news/computersecurity/2009-08-20-hacker-background_N.htm

Maiello, Brungo & Maiello, LLP. (n.d.). *Wi-Fi hotspots and liability concerns*. Retrieved from http://www.mbm-law.net/newsletter-articles/wi-fi-hotspots-and-liability-concerns/1229/

Na, C., & Rappaport, T. S. (2004, September 16). Measured wireless lan public hotspot traffic statistics. *Electronics*, *40*(19), 1-2.

Nazareno, A. (2011). *Free, public wi-fi can be dangerous to your credit card, bank accounts.* Retrieved from http://www.creditcards.com/credit-card-news/free-wifi-danger-credit-card-fraud-1273.php

O'Brien, C. (2010, April 3). On the hunt for naked Wi-Fi hotspots with a wireless detective. *San Jose Mercury News*. Retrieved from http://www.mercurynews.com/breaking-news/ci_14802784?source=rss

OnGuard Online. (2011, September). *Tips for using public wi-fi networks*. Retreived from http://onguardonline.gov/articles/0014-tips-using-public-wi-fi-networks

Phifer, L. (2010, March). *Top ten wi-fi security threats*. Retrieved from http://www.esecurityplanet.com/views/article.php/3869221/Top-Ten-WiFi-Security-Threats.htm

Potter, B. (2006, June). Wireless hotspots: Petri dish or wireless security. *Communications of the ACM*, *49*(6), 51-56.

Poturalski, H. (2012, January 19). Cyber attacks on the rise for smartphone users. *The Oxford Press*. Retrieved from http://www.oxfordpress.com/news/crime/cyber-attacks-on-the-rise-for-smartphone-users-1315445.html

Richmond, R. (2011, May 17). VPN for the masses. *New York Times*. Retrieved from http://gadgetwise.blogs.nytimes.com/2011/05/17/vpn-for-the-masses/

Roth, V., Polak, W., Rieffel, E., & Turner, T. (2008). Simple and effective defense against evil twin access points. *WiSec '08 proceedings of the first acm conference on wireless network security*. NewYork, NY: ACM. doi: 10.1145/1352533.1352569

Savitz, E., & Giordano, B. (2011, November 6). For hackers, there's a tempting new target: Your car. *Forbes*. Retrieved from http://www.forbes.com/sites/ciocentral/2011/11/06/for-hackers-theres-a-tempting-new-target-your-car

Symantec Corporation. (n.d.). *Online fraud: Pharming*. Retrieved from http://us.norton.com/cybercrime/pharming.jsp

Taylor, D., & McNeal, A. (2011). What's your fraud IQ? *Journal of Accountancy*, 212(5), 42-45.

Table 1

Types of Attacks

| Threat | Description | Information Gained | Solution |
|---|---|---|---|
| **Man-in-the-Middle** | User connects to a web server, and an attacker intercepts  communication between the two systems | Sensitive user information, including usernames and passwords | Ascertain which connections belong to the organization and are legitimate. Only transmit sensitive information over an HTTPS connection, a secured version of HTTP. |
| **Peer-to-Peer** | Target connects to the internet through the attacker's fake network | Online activity, access to folders and files on the victim's computer | Connect to "Access point (infrastructure) networks only". Disable the option to "always connect to preferred network" to avoid automatically connecting to a rogue network. |
| **Pharming** | Attacker creates a malicious web page which runs a browser based exploit | Personal information, such as the user's log-in credentials to various accounts | Examine the page and URL before entering any credentials. Look for misspellings on the page or in the address bar. |
| **Phishing** | Attacker installs software onto the victim's machine to distribute mass spam email | Access to the victim's email address book | Ensure computer has updated security patches, anti-virus software, and network interface card (NIC) firmware. |
| **Wardriving** | Attacker connects to an unsecured wireless Internet signal and installs a "sniffer program" | Customer credit and debit card numbers | Users need to set up secure wireless networks exclusively. Organizations should consider using wireless intrusion-prevention system (WIPS) products. |