

EXECUTIVE SUMMARY

- An unprecedented number of risks threaten users' safety at publicly available Wi-Fi hotspots, especially unmanaged hotspots where service is frequently free. In the past, the most common exploits required a degree in computer science – or at least a passionate pursuit of hacking as a hobby. Today, those same hacks can be performed by simply installing a browser plug-in and pointing-and-clicking through unsuspecting users' private lives.

- A well-managed network can limit the number of threats to users and reduce their exposure to hackers and snoops with active tracking, blocking, and monitoring. By properly configuring a network, maintaining diligence in evaluating the computing environment, and keeping up to date with the latest user threats, a managed service provider can limit threats to users and liabilities to the venue owner.

- There are steps that users can take and technologies they can use to mitigate much of the risk, but that asks a lot of users – especially as the population of Wi-Fi users shifts from tech savvy early adopters and power users to casual technology users with limited understanding of both the technology and the inherent risks.

- Increasingly, a network owner's ability to uniquely identify a potentially malicious end user is seen as a necessary safeguard to avoiding significant potential threats to national security and lawfulness. The trend in security-conscious countries is to require the WISP to identify the end user whether the service is commercial or free.



INTRODUCTION

The online world is no longer an inherently safe place. Hazards lurk for users at home, at the office, and especially on public networks, such as Wi-Fi hotspots. Phishing, hacking and other forms of fraud follow users wherever they connect. But open wireless

The number of threats that can compromise a hotspot user's identity, personal data, and system integrity continue to multiply

networks – especially ones that are unmanaged or poorly managed – present unique

threats that can be mitigated through diligence, both on the part of the network operator and the user.

The number of threats that can compromise a hotspot user's identity, personal data, and system integrity continue to multiply. Many threats are passive, with infected computers or mobile devices spreading viruses and malware through the local network.

THE RISKS

Public networks are by definition open networks, even though an account and password, payment, or other authentication means may be needed to gain access to the Internet service offered – or in the case of free networks, no barrier at all may exist to getting online. Data flows across the local portion of the network without any scrambling of the information that would prevent those with ill intent from intercepting it.

A private network uses encryption as one tool in preventing unwanted access, mitigating the worst attacks by shielding data from unwanted eyes and devices on the network from being reached by attackers. Because anyone can step up and use a public hotspot network, some exploits impossible or unlikely on a corporate (or even a home) network are in wide use in the public space.

Because of this, hotspot users face an unprecedented number of risks on public networks. The good news is that many users are now much better informed about those risks and taking security issues more seriously. Nearly every week, a mainstream newspaper or syndicated news story about the latest threat to Wi-Fi security educates millions of potential users as to the risks they face.¹ The U.S. government has also offered extensive advice to hotspot users that both educates and terrifies users.²

The bad news is that the population of less sophisticated users is growing rapidly with the explosion in Wi-Fi enabled consumer

Others are active, with thieves on a public network using freely available, often one-click software to gather private, financial, and identity information to use or sell to other parties.

A properly managed hotspot network can eliminate many of these risks and alert the network's operator – as well as the venue itself – to active threats, which in turn enables rapid response and eradication of the threat. In many instances properly managing the network also ensures that venue owners are meeting legally mandated government recordkeeping requirements, as well.

This white paper will cover: a) the risks users are exposed to when using open Wi-Fi networks, b) the actions that users can take to protect themselves anywhere they use a network, and c) the specific advantages of a well-managed network for reducing user exposure and improving the network experience for customers.

electronics gadgets such as smartphones, ereaders and gaming devices. This trend will likely continue, with the unaware masses outpacing the educated few on an ever-expanding basis, increasing the overall susceptibility to the most common exploits.

Each of these exploits has a solution – some of which a user can directly address in a few steps. Many of these same exploits – as well as some additional risks – can be severely mitigated by a managed services provider well-versed in designing networks to close some of the most common entry points that are used to exploit users, and monitoring for others.

“Free Public Wi-Fi” networks

Whenever you open a laptop or tap a mobile device in an area with a lot of people also using such equipment, you'll invariably see a network named “Free Public Wi-Fi” or some variant. Such networks are often the result of a quirk in Windows XP,³ which can be innocent (but annoying), but the networks can also be spawned by identity thieves looking to grab personal information from the unwary.

The urge to connect to “free” Wi-Fi is strong, but these networks are really computer-to-computer connections masquerading as an available network. This creates a direct connection to another person's computer, which presents a host of potential security issues. A user connecting to such a network could expose his



THE RISKS (CONT.)

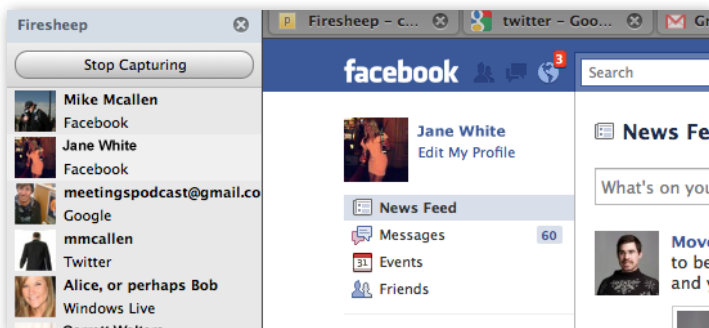
or her computer to viruses on the machine that's broadcasting the network name, or to direct attack from a malicious hacker. The best way to avoid this is for a user to disable the feature to connect to "ad hoc" networks within their operating system. Some Wi-Fi service providers also have connection managers that ignore computer-to-computer networks when looking for valid service networks.

Evil Twin

The "Evil Twin" is a network access point that broadcasts the same name as the legitimate venue network, but is intended to lure users to connect to it instead.⁴ Once a user connects, the evil twin passes traffic back and forth from the public Internet, while grabbing passwords and other private data. (The evil twin connects to the Internet through the real hotspot network or a cellular connection.) The evil twin can also substitute fake financial, ecommerce, and other Web pages at which a user may log in, bypassing secured safeguards present in those institutions and companies' Web sites. An end user would have a hard time telling an Evil Twin from the legitimate network, so they would be at the hacker's mercy. However, they can reduce their risk by using smart client software (applications provided by some Wi-Fi service providers to facilitate login and roaming) that may be able to identify a forged certificate and by ensuring the hotspot is a well-managed network that aggressively identifies rogue access points and triggers alerts or takes direct action against the unauthorized network.

Firesheep

The silly name of the software makes light of its serious threat. The Firesheep plug-in for Firefox, created by a security



Firesheep scans the local Wi-Fi network, identifies insecure connections in use by others on the network, and allows one click hijacking of such sessions.

The urge to connect to "free" Wi-Fi is strong, but these networks are really computer-to-computer connections masquerading as an available network

researcher to demonstrate weaknesses in social-networking and commerce sites, can steal someone's identity from the same network with a single click,⁵ whereas this degree of exposure was previously minimal due to the technical complexity of performing the procedure. Firesheep makes it point-and-click simple for even the most unsophisticated snoop.

Firesheep scans open networks for tokens sent by Web sites after a secure or insecure login that uniquely identifies that user for a session that might last minutes or days. The tokens are embedded in browser cookies, which are not encrypted if the Web pages being visited aren't also secured. Most web services like Facebook and Twitter are not encrypted by default – exposing users to this exploit just by visiting their site. A Firesheep user can click any active session collected during the scan, and connect to a Web site as that user. This allows a hacker to hijack the user's session and take control of their account, changing passwords, posting spam or performing other nefarious tasks.

Generic sniffing

Any public network is open to passive sniffing—or detection, storage, and analysis—of all the traffic passing over it that is not separately encrypted by a user or a service to which the user connects. Because many software programs, including email clients, may send passwords in the clear (unencrypted as plain text), a sniffer can retrieve information of great utility for identity theft and ecommerce fraud. Most email programs send all email in the clear – meaning that anyone within range can see the full text of every email a user sends on an open hotspot. The majority of these programs have an option to force secure connections for sending/receiving mail to thwart this exploit.

Infected computers

Many computers are laden with viruses that attempt to spread themselves to other systems on the same network whenever given an opportunity. This can happen if a user connects to a fake network, such as an evil twin or "Free Public Wi-Fi" network described above, or if computers aren't properly isolated on a hotspot network or the network itself isn't configured and monitored to protect against malware such as worms and viruses spreading through the network.



THE RISKS (CONT.)

Network hackers

More rarely, aggressive network hackers may take up residence on a public Wi-Fi network, most likely in a large venue in which many users are available for them to tumble. Such hackers will employ a variety of automated and manual techniques to break into other computers on the same network to install malware for later use or to retrieve or scan for private information, such as credit card numbers and account login credentials.

WHAT MANAGED SERVICE PROVIDERS CAN OFFER

As the number of uneducated users explodes, the onus for protecting the masses will fall increasingly on the network operator. While some of the risks cannot be mitigated at the network level, many of the most common can. A managed service provider must be diligent and focus on the design, implementation and maintenance of the network in order to reduce the risk to hapless users on the network. A side benefit of this kind of diligence is that it typically also improves the network's overall quality. This type of configuration is common among top commercial network providers, but is frequently overlooked by less experienced operators, especially in the deployment of free networks.

Blocking Firesheep

Until all popular sites encrypt all sessions following a login—a trend that is underway—Firesheep and similar automated scripts will be able to grab user session information to sidejack into an account – essentially for another user to pose as the original user unbeknownst to the original user or the service provider. But Firesheep activity can be blocked quite easily at a managed venue.

On a local level, the network manager can eliminate all peer-to-peer traffic over the network, prohibiting the plug-in from casually perusing unencrypted network packets on the shared portion of the network. This won't stop a real hacker using sniffing technology, but does reduce the efficacy of Firesheep in its current form.

Moving up the network further, by using advanced network address translation (NAT, which maps internal network addresses for users to multiple public Internet addresses) at the gateway, the web site would see the sidejacked session tokens emanating from two distinct IP address, and would expire the tokens. This effectively blocks the reuse of session tokens that identify users for many online sites. Since most public Web sites won't allow

the same token to be used simultaneously by two different Internet addresses, a properly configured NAT mapping implementation can foil the hacker from using any credentials they've captured via the plug-in.

In locations with largely unmanaged networks, a single public address is typically used to share access for all users in the venue. This approach doesn't trigger a Web site operator's system if a session is hijacked; in fact, this simplistic approach is an open invitation for Firesheep users and other hackers to exploit at will.

Preventing user-to-user traffic

Infected computers spread their viruses and malware across local networks indiscriminately. But even clean machines reveal too much about themselves on a local network. Users forget that firewall settings to share volumes and other information over a local network don't apply on a public one.

Another advantage to disabling peer-to-peer traffic – as described above – is that it prevents inadvertent or malicious communication among users,

Disabling peer-to-peer traffic prevents worms from penetrating, hackers from using probes to ferret out weaknesses and patrons from giving away information they intended to be private.

in addition to restricting snooping. This keeps worms from penetrating, hackers from using manual and automated probes to ferret out weaknesses, and hapless patrons from giving away information they intended to be private, including "shared" resources on their computer that were only designed to be shared with cohorts at work or home. This may not be a big deal if the user is sharing their music collection, but



WHAT MANAGED SERVICE PROVIDERS CAN OFFER (CONT.)

it can be a tremendous corporate liability if the shared directory on the hard drive includes confidential documents or trade secrets.

While some inexpensive home access points used at unmanaged locations include the ability to suppress peer-to-peer traffic, this feature is rarely enabled by default, and most unmanaged sites use the default setup outside of changing the network name (SSID). In some instances, even if the operator activates this feature the configuration may not be advanced enough to provide a full lockdown for devices on the network. There are significant control/management differences between \$60 access points and \$600 access points.

A sophisticated managed provider also looks for attempts to broadcast illegitimate traffic to an access point, often "poisoning" efforts that disrupt network operations. Clients engaged in such activities can be automatically dropped off the network and barred from regaining access.

Blocking all incoming connections

On a well-managed network, end users' computers shouldn't be exposed to malicious probes – within the network itself or from external sources. A managed provider uses firewalls and other controls to block arbitrary incoming connections, including those probing for weakness by masquerading as a response that was never requested.

Identifying and shutting down unauthorized access points

The "evil twin" technique relies on a malicious access point overwhelming the legitimate signals in the area. A managed provider actively monitors for rogue access points coming on line in the same radio frequency space.

If new broadcasts are discovered using the same network name, a managed provider can use techniques often employed in denial-of-service attacks by malicious parties, but in a targeted and legitimate manner. The managed network sends a command that forces the unwitting user's device off the evil twin.

The appearance of access points with different names is also noted and logged for potential forensic purposes in the event that a breach is later reported. In these instances, no immediate action is taken since many people now use portable hotspots, such as the MiFi or features built into smartphones.

This active monitoring and generation of alerts allows network administrators to take additional action, if necessary.

Monitoring and filtering traffic

Depending on the requirements of the venue and local law, a managed provider can engage in active filtering and monitoring of content to prevent illegal or inappropriate use of a network.

While content filtering has a bad name among many Internet users, in a captive network, some filtering may be necessary. In other cases, it may be a government or facility requirement. Frequently, government institutions require filtering of known adult sites, especially in environments that may also have children present. Or appropriate monitors/filters may need to be put in place to limit a venue's risk as it relates to enabling copyright violations (e.g., restricting torrent traffic).

Whatever the case, the software and services available for unmanaged locations requires constant care and updates to prevent public relations disasters when the wrong content is blocked,⁹ and to fulfill appropriate screening.

Government recordkeeping requirements

One of the biggest risks a non-managed venue faces are the recordkeeping requirements of several governments related to the prosecution of cybercrimes, child pornography, and media piracy, among other reasons such information is required.

United States: The Communication Assistance for Law Enforcement Act (CALEA) requires venues that meet the test for providing broadband service keep general records about Internet use, and be able to monitor use on presentation of an appropriate warrant. This requirement is not currently enforced for certain kinds of free access, but this is liable to change as the law doesn't exclude free service as such, and the trend worldwide is increased traceability of public network users, especially in high security locations such as airports.

Great Britain: The Digital Economy Act (DEA) passed in 2010 requires every hotspot, free or paid, to require registration or some other tracking method for identifying individual users. The law was initially intended for to help enforce copyright violation by rightsholders,¹⁰ but is expected to set key precedents for law enforcement as national security issues and the use of public networks in the operation of extremist groups come into focus.



WHAT MANAGED SERVICE PROVIDERS CAN OFFER (CONT.)

India: In February 2009, the Ministry of Telecommunications & IT distributed new rules to all Internet Service Providers in India that outlined the explicit steps that must be taken to ensure traceability of any user accessing the Internet over public or private networks. For public networks, such as Wi-Fi hotspots, at a minimum, the ISP has to generate login tokens and forward them to the user via SMS, in order to establish a known identity (mobile number) that is registered elsewhere. This was in response to the 2008 terrorist attack in Mumbai and suspicions that the organizers had used public networks to coordinate the attack.

Other countries may have greater requirements for tracking users, which is a burden on individual venues, and can result in fines or even criminal charges depending on the effort by a venue and the act in question by a customer. Managed service providers handle this fuss and meet the rules of which country or locality in which a venue operates. Multi-national service providers frequently implement the highest stringency requirement across all venues, ensuring the minimum compliance, and frequently providing a higher level of execution on a local level.

WHAT USERS CAN DO

But even with the considerable steps a sophisticated managed services provider can take to protect users, in many cases the users still need to take steps to protect themselves. People who use public hotspots – which constitutes a large percentage of the on-the-go population – need to be equally diligent to protect themselves against risk. Not all users will heed this advice – in fact, many will remain unaware of the risks and remedies – but these efforts are effective.

Deploy a personal or corporate VPN (Virtual Private Network)

First and foremost, all users on public networks should employ a VPN (virtual private network), which encrypts all the communications from any software on a user's computer to a server elsewhere on the Internet. This prevents sniffing of public traffic from being useful to anyone on the local network, as well as any compromised machines on the wired portion of the local network or even at the local Internet service provider.

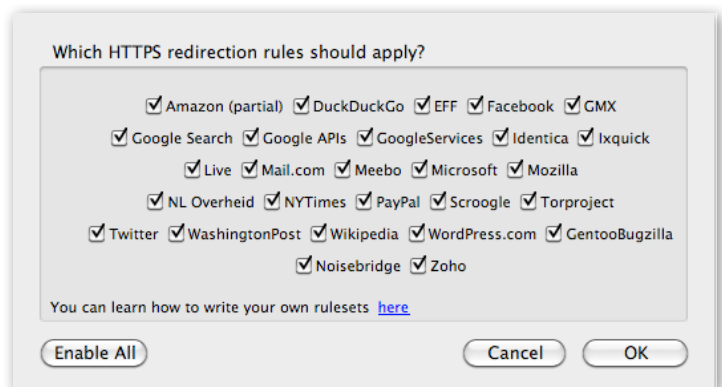
Corporations have long provided roaming users with VPN service that connects back to a company intranet or enterprise network, allowing secure remote use of a firm's internal resource. Some companies even install software that enforces use of the VPN: the VPN snaps into place the moment a user's smart client software connects to any network.

However, individuals and smaller firms don't routinely have access to this kind of information technology resource. Several companies offer for-fee and free VPN service. With these VPN providers, Internet traffic emerges at a privately owned data center, from which it traverses the rest of the Internet path to reach a destination.

Secure connections

Failing the use of a VPN, it is possible for a user to configure a computer or mobile device to connect to most common services using a secure method. Spurred partly by Google and by security researchers denouncing the problem, most major services allow fully secured connections, and many email clients automatically attempt to configure securely first. Further, many ISPs and mail hosts will not allow email to be sent from a customer using an unsecured method to minimize the risks of spambots leveraging unsecured servers.

The method of securing a connection can vary by each email client and mail provider or ISP. Google offers detailed instructions for many desktop and mobile email programs with its settings.⁶



Firefox browser users can install the free HTTPS Everywhere extension which ensures that only the secure version of popular sites are used while browsing [K]. (Similar extensions on other browsers visit the unencrypted sites first before redirecting to a



WHAT USERS CAN DO (CONT.)

secure site, rendering the tool useless for this purpose.)

Twitter allows secure access through its Web site, and recently added a preference in profile settings to require a secure connection for all Web sessions. In Twitter clients, users should check for a “https,” “SSL/TLS,” or “encrypted connection” box in the program’s preferences.



HTTPS Only Always use HTTPS
Use a secure connection where possible to encrypt your account information.

Most Google service are now available in secure form, including search, mail, and Google Docs. Using “https” instead of “http” at the start of the location is one way to reach secure sites. In Gmail, users can check a box in Settings to “Always Use https”.

Facebook recently added a secure option in response to Firesheep, government hacking in the Middle East, and other security concerns. Facebook users may log in on a trusted network (such as at home or work), visit Account Settings, and check a Secure Browsing option⁸.

FUTURE PROOFING A NETWORK

But running a network isn’t all about today: it also includes planning for what tomorrow will bring. Just like some venues were overwhelmed by the technical requirements and bandwidth use of the iPhone and other smartphones and mobile devices when they first appeared en masse a few years ago, new demands and requirements may spring up at any time. A sophisticated managed services provider works ahead of such developments to be ready for them.

Three upcoming changes are on the radar that any venue should be aware of as they consider their current and future hotspot plans.

Free networks with authentication

Some hotspot networks and chains have decided to forego usage fees in exchange for promoting use of a venue or selling advertising. However, many venues still need to ensure proper use of their networks, and have some measure of accountability by users. In most current implementations, this accountability has been lost.

Today’s common system of allowing arbitrary registration without confirmation of an account may not meet the needs of future

Firewall, virus, and malware protection

Users should also always have firewall, virus, and malware protection installed on Windows systems, where such software is readily available and regularly updated. By blocking inbound connections, monitoring programs on a computer for illicit outbound attempts, and scanning for invaders, users can avoid attacks and attacking others.

Such software is available for Mac OS X and Unix/Linux systems, but laptops running those operating systems have seen fewer exploitable weaknesses, and are used in much smaller quantities than Windows. Attacks still tend to focus on versions of Windows, although that could change.

Mobile systems remain vulnerable to attack because many platforms are relatively new, regularly revised, and frequently connected to public networks. A few smartphone platforms have tools for virus protection, but most rely on the operating system maker to keep the system safe, which is not a good assumption given the history of software platforms.

government recordkeeping rules, the ability to track misuse of a network, or a venue’s own interests in tracking users or offering different features for different patrons based on loyalty.

Various industry groups are still discussing alternate methods of providing complimentary access with any number of authentication methods to establish the accountability that appears to be increasingly required. These authentication methods can include an SMS message to a user’s phone, input of a credit-card number for validation (but not for charges), or use of third-party tokens that allow a user to employ a login for a service like Twitter or Facebook as part of his or her proof identity. By enforcing an authentication sequence that establishes a user’s unique identity (cellphone number, credit card, existing account), the location and service provider put themselves in the position of being able to accommodate the increasing traceability requirements that are gaining momentum around the world.

Requirements for network security

While public networks are typically open and require no security to use, that may change. In India, authorities cite uses by terrorists of open personal and work networks to exchange email anonymously as a reason for requiring security. A managed



FUTURE PROOFING A NETWORK (CONT.)

provider can overlay network passwords and facilitate such requirements if they come into play.

Changes in government recordkeeping

In response to terrorist and criminal activities, governments may abruptly impose new rules on Wi-Fi networks about security, recordkeeping, and filtering. Unmanaged locations, or poorly managed ones, may have difficulty implementing such changes quickly, and may need to disable their networks due to their inability to meet the requirements.

In response to the 2008 terrorist attack in Mumbai, the Ministry of Communications & IT in India issued a new set of rules and regulations around tracking the identity of all users accessing the Internet via public networks. Following the attack, suspicions grew that the terrorists coordinated their efforts via free Internet services that were readily available with no traceability.

New standards for better hotspot security

Watching and participating in the network standards process is part of any managed provider's job to make sure networks are ready for critical changes that may improve the efficiency and security. Currently, the IEEE 802.11u standard appears to be the one to watch¹¹.

The 802.11u protocol would allow a hotspot to offer a secure connection to a customer trying to connect, presenting information about available networks beyond just the unreliable network name. This standard would prevent the "evil twin" and "Free Public Wi-Fi" exploits or network configuration issues from affecting users. It also provides encryption specific to each and every user, making it much more difficult to sniff other users' traffic and capture anything useful.

The protocol would also make it easier for a roaming user – one carrying a mobile device as they walk or work around a venue – to reconnect to the network in a secure and seamless fashion, better than today's efforts.

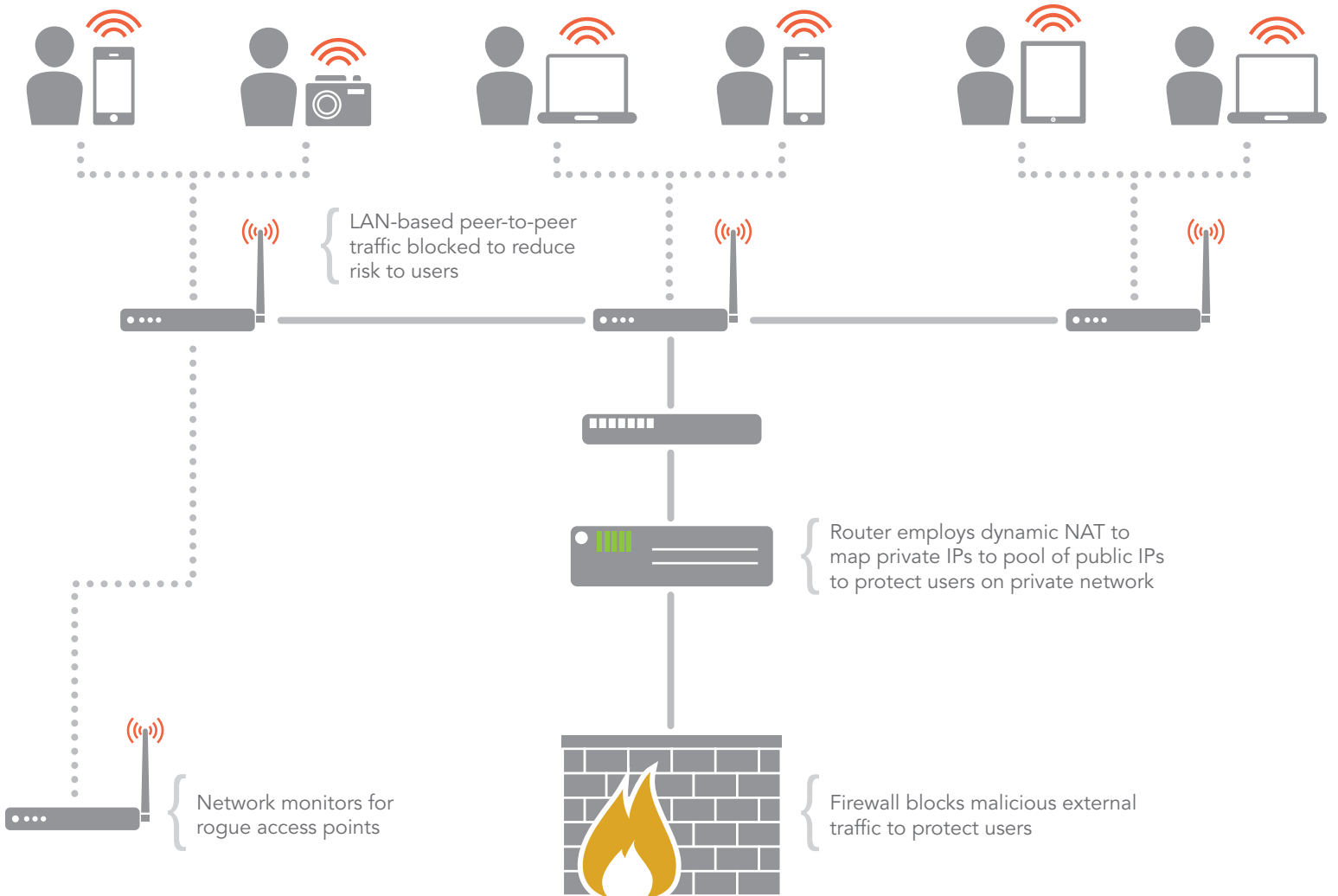
MITIGATING RISK WITH THE RIGHT PARTNER

Planning, implementation and monitoring are the only way to keep a Wi-Fi network safe. Venue owners and operators don't need to become Wi-Fi experts to keep their networks up to date and safe for users. While users must become better informed in this area of increased risk, venue owners can turn to best-of-class managed service providers to take the problem seriously now and when future issues arise.



Key Security Safeguards in Managed Networks

PRIVATE LAN NETWORK



PUBLIC WAN NETWORK



References

- 1: <https://www.nytimes.com/2011/02/17/technology/personaltech/17basics.html>
- 2: <http://www.onguardonline.gov/topics/hotspots.aspx>
- 3: <http://wlanbook.com/free-public-wifi-ssid/>
- 4: http://www.pcworld.com/article/120054/does_your_wifi_hotspot_have_an_evil_twin.html
- 5: <http://codebutler.com/firesheep>
- 6: <https://mail.google.com/support/bin/topic.py?hl=en&topic=12913>
- 7: <https://mail.google.com/support/bin/answer.py?hl=en&answer=74765>
- 8: <https://www.facebook.com/blog.php?post=486790652130>
- K: <https://www.eff.org/https-everywhere>
- 9: <http://boingboing.net/2008/02/13/david-byrne-i-was-bo.html>
- 10: <http://www.zdnet.co.uk/news/regulation/2011/01/24/vaizey-sets-isp-costs-for-chasing-suspected-web-pirates-40091535/>
- 11: http://www.ieee802.org/11/Reports/tgu_update.htm

Free VPN providers

- AnchorFree <http://anchorfree.com/>
LogMeIn Hamachi2 <https://secure.logmein.com/products/hamachi2/>
SecurityKiss <http://www.securitykiss.com/sk/index.php?m=Download>

Paid VPN providers

- HotSpotVPN <http://www.hotspotvpn.com/>
StrongVPN <http://strongvpn.com/>
WiTopia <http://www.witopia.net/welcome.php>

