in this issue >>> V. 2.10

*Kismet Smarter Wi-Fi Manager*

*Wi-Fi Security & Privacy: Encryption*

*Wi-Fi SSID Opt-Out UPDATE*

*Public Wi-Fi Threats*

*Self-Destructing Cookies*

TOUCHPOINT
INTERNATIONAL DEVELOPMENT GROUP, INC

TOUCHPOINT
INTERNATIONAL DEVELOPMENT GROUP, INC

A Bi-Monthly Snapshot into Emerging Threats and Trends

# Digital Update

current topics >>>

## In the News:

- Social Security Website to Allow Stronger Authentication
  - Krebs On Security
- Protect Yourself from Modern Phishing Attempts
  - Lifehacker
- Massive Vulnerability in Windows Defender Leaves Most PCs at Risk
  - Ars Technica
- Mac Users Installing Popular DVD Ripper get Nasty Backdoor
  - Ars Technica
- Android Phones Covertly Listening to Inaudible Tones in Ads
  - Ars Technica
- Greyhound.com: The Site With the Worst Password Policy on the Internet
  - Ars Technica

# Kismet Smart Wi-Fi

## *Managing Mobile Wi-Fi Networks*

Managing how your smartphone interacts with Wi-Fi networks is extremely important. Since you carry your phone everywhere, it can track you everywhere. Leaving your Wi-Fi on enables this tracking and sets you up for things like an “evil twin attack” (see the last page for a description of this attack). The easy solution to many of these problems is to simply turn your Wi-Fi off when you leave home, but this step is easy to forget. Kismet Smarter Wi-Fi Manager can help.

Kismet Smarter Wi-Fi Manager is only available for Android devices. This app will turn your Wi-Fi on and off for you so you don’t have to worry about it. To do this the system works by using geofences, geographic boundaries, and requires that you allow Kismet to access your location as defined by nearby cell towers. This means that the app will keep Wi-Fi turned off when you are running errands, but as soon as you get back home Wi-Fi will automatically turn back on and your device will connect to your local network.

The application also allows you to create multiple whitelisted networks and geofences, allowing you to trust your home, office, and any other frequently-visited locations where you use Wi-Fi. Kismet also has a lot of other functions that let you customize your Wi-Fi usage. For example, you can create a list of networks that your phone will ignore, regardless of the geofence you are in. We found this to be extremely helpful in residential neighborhoods where Wi-Fi networks overlap. Even though Wi-Fi is on it will ignore all of the other networks.

Kismet Smarter Wi-Fi Manager also allows you to set time boundaries, during which Wi-Fi is turned off. This might be helpful if you don’t want Wi-Fi on at all during certain times, regardless of where you are. Finally, the app will let you manage Bluetooth—an extremely helpful feature.

We really liked the convenience of not having to think about turning Wi-Fi off and we highly recommend Kismet Smarter Wi-Fi Manager, which costs $1.99, and is available through Google Play Store.

*Active Self Protection >>>*

# Wi-Fi Security & Privacy: Encryption

One of the most important steps you can take to secure your Wi-Fi network is to encrypt it. Wi-Fi is nothing more than a radio signal, so intercepting it is a trivial matter. All it requires is a computer, an antenna capable of monitor mode, and some relatively simple software. Encrypting your signal does not prevent it from being intercepted, but it does make sure that all the packets are unusable. There are four basic levels of encryption that you might find on your router: no encryption, WEP (RC4), WPA (TKIP), and WPA2 (AES-CCMP).

Wired Equivalent Privacy (WEP) is not recommended under any circumstances. WEP uses the RC4 stream cipher to encrypt traffic and only supports a password of up to 5 or 13 characters. This protocol is very old and has been broken for a long time. The next option is WPA (Wi-Fi Protected Access) which uses TKIP (based on RC4) to encrypt traffic. WPA is stronger, but it's foundations are weak because it is based on the cipher used by WEP. It is broken and no longer considered secure. The final encryption option is WPA2 (Wi-Fi Protected Access, 2nd Generation). WPA2 uses a modified version of AES often referred to as AES-CCMP to encrypt traffic. This protocol is much stronger than WPA and is considered to be secure, but if your router is older it may not support WPA2. If that is the case you will have to go with WPA for now, but make sure to upgrade your router as soon as possible!

It is important to remember that encryption is only as strong as the password that protects it. When you set up your WPA2 encryption, be sure to give it a strong password (WPA and WPA2 passwords may be between 8 and 63 characters). A strong password protects your traffic from anyone attempting to intercept it. It also prevents others from using your Wi-Fi. It is important to remember that too much bandwidth on your network will slow your internet speed, and anyone with access to your network may use it to conduct illegal activity, from downloading pirated movies to visiting other illegal sites. Secure your router today with WPA2 encryption!

## Upcoming Events:

**Law Enforcement Intelligence Units**

*May 1-5 2017, Bloomington, MN*

**Associated Locksmiths of America Expo**

*June 16-22 2017, Rosemont, IL*

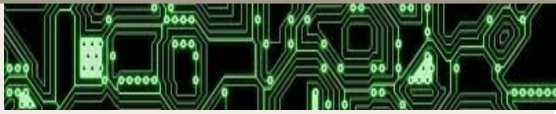
**National Technical Investigators' Association (NATIA) Annual Conference**

*July 12-23 2017, Tampa, FL*

**BlackHat USA**

*July 22-27 2017, Las Vegas, NV*

*The easy button >>>*



# Wi-Fi SSID UPDATE

## *New Opt-Out Technique*

In the last issue of the Digital Update we discussed Wi-Fi SSID privacy and security techniques. One of these techniques was adding "_nomap" to your SSID to prevent it from being collected by Google and referenced on various Wi-Fi mapping services like Wigle.net. Since that issue we have learned of a new technique that can prevent your Wi-Fi network from being mapped by Microsoft, and we feel it is important to bring it to your attention.

Microsoft introduced "WiFiSense" in Windows 10 which allows your Windows 10 computer to share you login information with your friends. While this has some obvious security and privacy problems, there is another important feature we feel needs to be addressed. Microsoft will also geographically reference these networks unless you tell them not to in your SSID. In order to opt out of this Microsoft requires that your SSID have the word "optout" somewhere in the SSID.

Since Google and Microsoft both require different opt-out procedures, we recommend including both of these terms in your SSID. Google requires that the LAST portion of the SSID be "_nomap" but Microsoft doesn't care where you put the word "optout". So, using the example from the last issue, "Johnson_wifi" would become "Johnson_wifi_optout_nomap"

This ensures that you are opted out of both services.

# Public Wi-Fi Threats

## *The Dangers of Using Untrusted Networks*

Securing your home Wi-Fi network is relatively easy. However, staying safe when using public networks can be much more difficult. You don't control the hardware that manages these networks, so you don't really know what is happening behind the scenes. Before using public Wi-Fi you should consider the following threats.

> **Evil Twin Attack**: In this attack, the malicious actor will first analyze your Wi-Fi probes—the requests your phone and computer send out when looking for known networks. The attacker will then set up a Wi-Fi network with the same SSID as one of your trusted networks. Your device will connect to it automatically, and all traffic will then be sent through this "evil twin" network. Devices like the Hak5 Pineapple can create these networks automatically. In another instance the attacker can simply create a network with a name similar to legitimate networks in the area. For instance, the Wi-Fi networks in the Charlotte Airport are named "CLT Free WiFi". An attacker might make a very subtle change and name their network "CLT Free Wi-Fi". Many unsuspecting people would connect to this network, believing it to be the legitimate airport network. To make it even more believable, the attacker may even create a login page that requires you to accept terms and conditions, just like the airport's real network.
>
> **Packet Sniffing**: In this attack, your unencrypted Wi-Fi traffic is collected incredibly easily with a very small amount of technical knowledge. An attacker can view your traffic and steal your personal information by passively listening to your unencrypted traffic.

Even if none of these attacks happen to you, connecting to a public Wi-Fi hotspot exposes you to a lot of risk. First, even if the network you are using is completely legitimate, the network operator still has access to all router logs. These logs will contain each user's MAC, the time they were connected, and some information about the sites that they visited. This information may then be spilled in a breach or stolen by a rogue employee. Even leaving your Wi-Fi turned on can expose you to risk, because your phone and laptop are always searching for Wi-Fi. This means every router in your vicinity can see the names of the networks you routinely connect to, and, as we saw last week, these are geo-referenced on sites like Wigle.net.

In the next issue of Digital Update we will provide you with some actions you can take to stay safe on public networks. In the meantime, try to avoid using them!

# *Self-Destructing Cookies for Firefox*

Cookies are a necessary evil of the internet. For sites to function they must place cookies on your computer. Cookies are used to remember login information. They are also used to remember pages you've visited and items you have put in your shopping cart. This is how you can stay logged into your Amazon account and keep all of your items saved in your cart, even as you navigate from page-to-page.

However, Cookies can also be used for malicious purposes. A huge percentage of websites will install cookies that track you on any other sites you visit. These cookies see the items you are interested in and purchase, the news stories you read, and the accounts that you login to. This large-scale collection is extremely invasive and is used market items more effectively, or to make a richer profile on you that can be sold to advertisers.

Firefox can be setup to delete cookies and other history when the browser is closed, but the Self-Destructing Cookies add-on takes a more aggressive approach. This add-on deletes cookies on a "per-tab" basis. For example, if I have three tabs open and close two of them, Self-Destructing Cookies will delete the cookies that those tabs installed on my computer. We like this because it means you don't have to close the entire browser to keep your cookie folder clean.

coming soon >>>

## *In Future Issues...*

***Internet Browser Comparison***

- ⇒ ***Chrome, Firefox, Opera***
- ⇒ ***Mobile Browsers***

***Firefox Setup Review***

***Browser Extensions***