Celebrating 20 Years of Service 1994-2014

SWCP Portal

July 2014

Free, easy, and convenient, but for whom?

Dangers of Free WiFi

***Mark Costlow**, President*

Ars Technica tech news site recently **warned** that **public WiFi hotspots** can pose a security risk to users. It's not that hotspots are themselves insecure. It's the way most computers, tablets, and phones handle WiFi logins that poses a potential danger.

AT&T and **Comcast**, among others, are promoting large networks of WiFi hotspots free for their customers to use. For example, AT&T's free WiFi hotspots are available at McDonald's and Starbucks. When you see the "`attwifi`" network at any of these places around the country you can log in with your AT&T login. The same goes for Comcast's "`xfinitywifi`".

Once you have logged in to one of these networks, your computer or tablet probably saves the **login information** so you can reconnect to these networks without entering a password the next time you are near one of their hotspots. This is the window that can let the bad guys in.

What the criminal can do to the unsuspecting device owner is set up his own WiFi hotspot using the network name "`attwifi`" or "`xfinitywifi`". But the crook's hotspot has some tricks up its sleeve. First, it allows you to connect regardless of what username and password is entered. Bingo, the bad guy has got your AT&T or Comcast login information. Often, this alone would be enough info to cause damage, either vandalism of your online life or identity theft.

But even more insidious, this low-life and his illicit hotspot have become a **man-in-the-middle**. He now has the power to intercept *all* of your communication, including emails, websites you visit, and possibly account passwords sent to other websites (Facebook, Twitter, your bank, etc.) They can also inject anything they want into the webpages you are looking at. So even if you stay away from shady sites which might have malicious code on them, the man-in-the-middle could slip them undetected into the flow headed to your browser anyway.

Protocols such as **SSL** (indicated by the little padlock icon in your browser when you are on a secure site) are intended to withstand these man-in-the-middle attacks. However, the bottom line is that a bad guy in the midst of your communications has enormous power to try and subvert *any* security that would otherwise be in place. He's not just able to snoop on your packets, he gets the chance to change each one as it passes through his evil access point.

How can a person protect themselves against this? The best advice would be to never use free public WiFi hotspots. That's not really practical though – they are simply too useful to ignore. The next best thing is to configure your device NOT to "remember" those WiFi hotspots. Or, after you use one, specifically tell your device to forget it. Sadly, this is almost impossible to do on Apple phones and tablets.

And finally: never, *ever*, log in to your bank or credit card web site through a public WiFi hot spot. ***Never***.

From main dish to modern menace

The Secret Life of Spam

Spam originally was, and still is, a kind of lunch meat made largely from spiced ham, served to GIs in the Pacific during World War II. Today the term more often refers to **unsolicited bulk email**, after a famous 1970 pre-internet Monty Python sketch about a cafe that featured mostly spam in every dish.

Continued on back

Continued from front

To early users, the name seemed apt due to the large amount mixed in their email. But there can be many forms, from physical junk mail to electronic, infesting everything from blogs to telemarketing calls to TV to web searches. Yet **email spam**, in particular, is a major clogger of bandwidth, ranging from *85%* of all email volume worldwide down to *66%* in some places where hard efforts are being made to fight it.

Spam is more than just a nuisance, but a serious threat. The California legislature estimated that in 2007 alone, dealing with spam cost the US *$13 billion*. While much spam remains advertising for real, often shoddy, counterfeit, or illicit products such as pharmaceuticals, others are outright scams, carry viruses, or are phishing attempts to steal personal information or take over computers. So warnings are constantly being issued about the dangers of opening or even worse, responding to, unsolicited ads.

A huge effort has been mounted to create **spam filters** using everything from subject-line keywords to Bayesian logic pattern detectors that can learn from user choices. Multiple filters, each working slightly differently, also help; so SWCP's suite of free filters includes **SpamAssassin**, **Spamprobe**, **white and black lists** (to allow email to pass unimpeded or block it completely), and **keyword filtering** as well.

However, since spammers exist in the same underworld as virus writers and hackers, little is known of how it all functions. Recently, however, researchers from UC Santa Barbara and Aachen University have set up a series of **online experiments** designed to ferret out the secrets of how they operate.

They used "honeypots" to lure spammers in and track the results. By setting up their own domains, servers, fake websites and users, the researchers have discovered a **division of labor** among spammers. This specialization creates a secret, prosperous **marketplace economy** with many players that provide each other with the essential services to make it all work.

Spam ecology

Individual spammers run unique **spam campaigns**. These operations send out batches of email with particular themes and little variation. A single successful campaign can generate revenues between *$400,000* and *$1,000,000*, so there's certainly incentive. To run a profitable campaign, a spammer needs: 1) a list of valid email **addresses** of potential victims, 2) **content** in the message that not only avoids being snagged by filters but also hooks the victim quickly, and 3) a way of **distributing** spam, such as a **botnet**. The illicit goods they push also require websites, shipping facilities, and online payment processors.

Usually each of these functions is done by a separate party. Spammers generally buy lists of addresses from email harvesters and rent botnets, but occasionally they perform one of these other tasks themselves. Reputation apparently counts a great deal, and there's customer loyalty, too, as the same suppliers often cooperate on a number of campaigns.

Email addresses can be gathered from postings on the web using **webcrawlers**, or bought on the black market, in which case they may be used by various spammers. Most email harvesters, suprisingly, come from Germany. But wherever the lists are from, spammers tend to use the same ones for years.

Gaming websites are by far the biggest sources of addresses, followed distantly by online forums, while blogs and private webpages provided the least. Interestingly, some spam was sent to generic addresses at the spamtrap sites, and much more to be relayed on to gmail or other big providers to evade detection.

Spam is usually distributed by means of a **botnet**, a network of zombie computers that have already been taken over through a previous campaign. These botnets are hosted in different countries all around the world, usually not the spammer's own.

Addresses from lists can be used in spam **Reply to:** fields. So if you suddenly get a "Mail undeliverable" message for spam supposedly sent by you, it probably doesn't mean you've been hijacked but rather, "**joe-jobbed**": it's just a ploy to get you to respond.

Continuing questions

A lot of spam is simply bizarre. Much contains chunks of text taken randomly from books, most likely to evade filters. But a good deal doesn't seem intended to sell anything, or contain links or hidden malware.

Their purpose remains a mystery. Guesses range from goofs by novices to attempts to provoke a reply, filter-evading trial-runs, or hiding encrypted messages. The safest thing remains to delete them untouched. But if you've a question, feel free to check with SWCP Tech Support. We're all in this together.

Southwest Cyberport

New Mexico's Expert Internet Service Provider since 1994
505-243-SWCP (7927) ◉ **SWCP.com** ◉ **Help@swcp.com**
5021 Indian School NE, Suite 600, Albuquerque, NM 87110

Portal *editor/chief writer, Jay Nelson* **jnelson@swcp.com**