# CALIFORNIA STATE SCIENCE FAIR
# 2014 PROJECT SUMMARY

**Name(s)**
**Manaal A. Sayed**

**Project Number**
34629

**Project Title**
## Ethical Hacking: Invisible Sharks in Cyberspace

**Abstract**

**Objectives/Goals**

It only takes one lost email or online banking password, or one hacked Facebook account to turn your world upside down. The average consumer does not realize the fact that persons with a malevolent intent can access everyday consumer personal information using a Man-in-the-Middle (MITM) attack. This attack is oblivious to the victim. My hypothesis is that an attacker can not only obtain usernames and passwords from a regular HTTP website accessed over a public Wi-Fi network, but an attacker can also take advantage of the insecure way in which SSL is implemented in HTTPS websites.

My objective is to not only make people aware of the dangers that exist at public Wi-Fi networks, but also to make people aware that Secure Socket Layer (SSL) - one of the world's standard forms of commercial encryption - is not a complete solution to the problem.

**Methods/Materials**

In order to test my hypothesis, I simulated the environment of a public Wi-Fi network using a wireless router. I connected a workstation as an attacker, along with another windows laptop, an iPad, and a windows tablet as victims, to the wireless router. From the attacker machine, I initiated a sniff attack on the network. From each victim device, I was able to access several regular HTTP and SSL encrypted HTTPS websites using different browsers.

The experiment was based around a man-in-the-middle attack, where the system attempted to sniff and obtain data from insecure and secure websites. The attacker used software, such as Cain and Abel, Wireshark and SSL Strip to compromise the information sent between the user and the supposedly secure webpage.

**Results**

The attacker was able to retrieve the passwords from all the regular, insecure websites using HTTP. I was also able to obtain data from the SSL encrypted websites, such as PayPal, Gmail, Yahoo, and Facebook, including credit card numbers and control of several email accounts.

**Conclusions/Discussion**

Based on my results, I conclude that user passwords are not secure over a public Wi-Fi. There is a real and tangible threat to HTTP and HTTPS websites from attackers. There are several highly probable solutions, which will require additional testing by internet security companies in order to prove their validity in today's environment.

**Summary Statement**

This experiment was conducted to determine the vulnerabilities of obtaining personal user data at a public Wi-Fi network using secure and insecure channels, and the probable solutions to these problems.

**Help Received**

I was helped by Mr. Charles Pascal - Amateur Radio Group Chairman at California Yacht Club - to understand and simulate public wireless networks.